INFORMATION CONTROL:
PRESERVING THE ADVANTAGE

BY

LIEUTENANT COLONEL CASEY M. BEARD

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2015

APPROVAL

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

Dr. Everett C. Dolman

Colonel Michael V. Smith, PhD.

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Lieutenant Colonel Casey Beard was a 2001 graduate of Clemson University, where he majored in Chemistry. He is a space operations officer with experience in nuclear operations, satellite communications, space control, and operational level command and control.

ACKNOWLEDGMENTS

This project consumed a vast majority of my life for nearly six months, and I would be remiss without recognizing and showing my deepest gratitude to those who made this thesis possible. First, Dr. Everett Dolman and Colonel Michael V. Smith sacrificed an incredible amount of time to guide me along the way, greatly enhancing my process of discovery. I cannot thank them enough for their patience and commitment. Additional words of thanks go to Mr. Brad Shaffer (a true space warrior, mentor, and patriot) for his lasting influence and Captain Stephen Ziegenfuss, who spared personal time to review and provide valuable feedback on my introduction.

Above all, I would like to thank my wife and children. Put simply, this thesis would not be possible without their love, support, encouragement, and joy. I do not have the words to express how blessed I am to have them in my life. To my family, I can only say thank you, I love you, and I dedicate this paper to you.

ABSTRACT

The world has changed, and so must the character of war. The US defense establishment remains rooted in a paradigm that emerged after the dissolution of its long-term rival, the Soviet Union. However, prevailing assumptions underscoring America's approach to power projection and employment are quickly losing their relevance. After the Cold War, the world witnessed mass proliferation and commercialization of information systems, creating complex (and man-made) information environments upon which US national security now wholly depends. Moreover, this reliance developed in a relatively permissive operational environment, raising expectations on the availability of information networks and subsequently shaping US defense policy, strategy, and doctrine. As the twenty-first century progresses, potential adversaries—having spent decades observing US operations—now have the capacity to neutralize US advantages, particularly through the denial or disruption of space and cyberspace networks, the backbone of information environments, or infospheres.

If the United States intends to preserve its way of life and ability to project power in the twenty-first century, it must deliberately establish a comprehensive and *prioritized* information control strategy that serves as the foundation for a new way of warfare. To gain the advantage in tomorrow's war, an information control strategy should first focus on the identification and protection of the infospheres that enable national endeavors. By extension, adoption of integrated space and cyberspace control strategies (designed to secure freedom of access, maneuverability, and exploitation of the infospheres they form) sets the necessary condition for information control and preserves America's power in the twenty-first century.

CONTENTS

Illustrations

Figure

INTRODUCTION

The character of war must change. The world has experienced a radical growth in information collection and dissemination technologies, allowing unprecedented access to near instantaneous information through global communication networks and the information environments they form, constituting the hallmark of the Information Age. However, the rapid proliferation of information systems and a dangerously unavoidable reliance on their capabilities to execute national and joint military operations create susceptibilities that are not completely known or appreciated. Moreover, the United States will not be able to achieve its strategic objectives in future wars unless it deliberately and collectively defines and secures the information environments it employs. This realization demands a new way of warfare: a comprehensive, global, *and prioritized* pursuit of information control, warranting its own strategy, distinct from yet synchronized with other national and theater operations.

The purpose of the following analysis is to highlight and evaluate two interrelated problem sets stemming from the emerging complexities of Information Age warfare. The first problem set, more overarching in its scope, centers on national and joint approaches to military force projection and application in the twenty-first century. As it stands, the US military, largely unchallenged since 1991, is entrenched in Industrial Age paradigms and is therefore not postured to adequately plan for or implement information control measures commensurate with the developing strategic landscape. The second problem, a subset of the first issue, involves the outmoded (and convoluted) strategies, policies, cultures, and organizations that define current US military space operations, effectively restricting the US military's ability to operate in increasingly contested information environments. At the same time, the US defense establishment emphasizes cyberspace as the central component of information environments while failing to view global space architectures in a similar vein. In reality, military space capabilities are inherently *informational* and form the original foundation of modern information environments. In fact, deficiencies in US military space operations epitomize the larger issues surrounding the joint force's purported inadequacies relative to the evolving strategic environment.

Ultimately, *if the United States seeks to preserve its desired way of warfare in the twenty-first century, it must adopt a global information control strategy that identifies and secures access to the information systems and networks empowering national security endeavors*. By extension, *the development of an information control strategy invariably demands the adoption of an associated space control strategy*, designed to identify and secure access to space systems that collect and disseminate information in fulfillment of a particular strategy's requirements. Most significantly, space and information control strategies are *not* confined to the space community as their attainment represents the predominant joint imperative for modern warfare. Consequently, the US space infrastructure provides a useful model for establishing a baseline framework for Information Age warfare and evaluating opportunities for conceptual and organizational transformation across the joint force.

Discussion of the Problem Sets

Prevailing strategies, doctrines, and force structures compound the challenges associated with the realities of Information Age warfare. Western concepts of force application and war assimilate under an Industrial Age paradigm, characterized by linear, reproducible, and efficient processes aimed at quantity, mass, and concentration of tangible strength to defeat an adversary.[1] In contrast, Information Age interactions value dynamic, open loop, qualitative, and non-linear approaches to solving problem sets and conflict, many of which—on the surface—seem to contest conventional, Industrial Age perspectives.[2] Subsequently, cognitive clashes ensue in an Industrial Age defense establishment as it struggles to recognize, understand, and appreciate Information Age nuances and implications on warfare; translate these nebulous concepts into action; and adjust or adapt appropriately, all while building upon an Industrial Age base. Consequently, a dichotomy exists between force development, structure, and application, as US military services organize and train under Industrial Age precepts yet increasingly equip warfighters with Information Age technologies and weapon systems. In essence,

[1] Keith L. Shimko, *The Iraq Wars and America's Military Revolution*, (New York, NY: Cambridge University Press, 2010), 10.
[2] John E. Rothrock, Edward F. Smith, Jr., and John F. Kreis, *The Industrial Age Versus the Information Age: Rethinking National Security in the 21st Century*, IDA Document D-2536 (Alexandria, VA: Institute for Defense Analyses, 2001), 5.

the United States military maintains an Industrial Age mindset for national defense in an Information Age world.

At its core, the role of information in warfare remains unchanged between the Industrial and Information Age—the nature of war consists of humans seeking to gain the advantage over their enemies, and information remains fundamental in supporting strategies and decision-making to that end. However, the Information Age *has* changed the importance of information *from a system or warfighting capability perspective*. While humans can theoretically operate with limited information (or with information saturation), the systems they procure and employ in the twenty-first century embody the networked technologies descriptive of the age, requiring access to information environments to operate properly (or at all). After the first Gulf War, the US military experienced a boom in information systems and networks, inexorably stemming from an insatiable supply-demand relationship between information, information systems, and decision makers at all levels of war in a perpetual attempt to reduce friction. Concurrently, though, weapon and command and control (C2) systems increasingly relied on net-centricity to function, empowering strategists to harness the force-multiplying benefits of cross-domain solutions yet revealing a blatant susceptibility unique to Information Age warfare. Indeed, the information environment (described later in the modified form of an *infosphere*, a product of the Industrial Age and artifact of the Information Age) now serves as the backbone of US power projection and functions as the connective tissue for cross-domain operations.

From a political standpoint, the asymmetric advantages afforded by net-centric operations greatly influenced public perception and expectations on the proper conduct of war. The overwhelming success of precision-guided munitions (PGM) during Desert Storm, so widely reported on during the conflict, generated a consuming standard for little-to-no collateral damage and thus a more judicious use of force in subsequent conflicts. As a result, public observations—more prevalent due to newly accessible information sources such as the Internet, cell phones, satellite communicates, et al.—translated into political guidelines, contributing to a seemingly inevitable progression toward more streamlined, highly technical, networked forces integrated across multiple domains. Accordingly, *the United States military now expects to project and employ*

force via the concentration of lean, disparate, and geographically dispersed units at a specific time and place for precision engagement.

The emerging way of war transpired under relatively permissive conditions, however, potentially leading to a premature acceptance of its validity as a model for twenty-first century warfare. Since the end of Desert Storm (and the near-simultaneous end of the Cold War), the United States advanced its transformative concepts while engaging militarily and technologically inferior opponents. In many ways, operational situations of relatively low intensity provided a sanitary laboratory for US forces to exploit technical solutions with minimal resistance, inevitably leading to potent and promising results on the battlefield. As a result, and despite increased awareness across the US government, joint forces enjoyed the benefits of planning and executing real-world operations largely under the assumption that information environments were always available. Today, information operations, codified in joint publications, are integrated with theater campaigns but are not bound under an overarching strategy that seeks to comprehensively identify and control access to the information systems that comprise enabling information environments. In the end, the rapid expansion of global information networks, the inherent complexities of Information Age precepts, and an almost unchecked employment of information-driven technologies in limited wars created a situation in which the joint force does not fully understand or appreciate the intricacies involved in enabling its desired way of war. Therefore, the first problem set is articulated accordingly:

- **Problem Set #1:** *The joint force is not designed or prepared to gain and maintain information control on a global scale and is therefore not postured for victory in the Information Age*.

The second problem set, directly related to the first, deals with the US military's perspectives on space in relation to Information Age warfare. Specifically, extant space doctrine, organization, training, materiel, leadership and personnel, and facilities (DOTMLPF) formed around two diametrically opposed geopolitical contexts. Historically aligned with Cold War policies and nuclear deterrence, the US space infrastructure reached a convergence with conventional warfare during Desert Storm in 1991. Space capabilities achieved a significant breakthrough during the first Gulf War,

and the dissolution of the Soviet Union months later only magnified space's potential. Space force enhancement (SFE) capabilities such as position, navigation, and timing (PNT); missile warning; satellite communications (SATCOM); terrestrial and space weather; and even exquisite intelligence collection produced overwhelming advantages for joint forces in Iraq. Desert Storm's tremendous success prompted service and joint components to expand the force multiplying capabilities afforded by space systems, creating a vicious supply-demand cycle that continues today. In telling fashion, Arthur C. Clarke described Desert Storm as "the world's first satellite war."[3]

After Desert Storm and the Soviet Union's abrupt collapse soon thereafter, one key strategic perspective emerged, fueled by a second key strategic reality, both of which cemented space operations in its current paradigm. First, national, service, and joint components suddenly viewed space as a dominant force enabler, placing increased importance and requirements on its collection and dissemination capabilities. Second, the Soviet Union's removal from the international scene eliminated the only near-peer competitor who could threaten US access to or operations in space. Consequently, space capabilities flourished in the emerging Information Age while remaining virtually unchallenged. Additionally, and just as significantly, US space policy and strategy remained convoluted and stagnant, tied to closely calculated international norms that categorized the domain as a universal sanctuary—there was neither competition nor a threat, so US access to space continued unabated while a clear strategy languished. This perspective further relegated the attainment of space superiority to a capability-based measurement rather than an operationally focused endeavor. In other words, space control and superiority became presupposed conditions—de facto states—rather than strategies involving *active* attainment and sustainment within non-permissive conditions. These strategic perspectives and operational realities influenced service and joint paradigms, generating a US space DOTMLPF that is optimized for delivering SFE capabilities in a relatively benign environment.

[3] Quoted in Everett C. Dolman, *Astropolitik: Classical Geopolitics in the Space Age*, (London, Frank Cass, 2002), 152.

More than ever before, US national security—and even national and global prosperity—wholly depends upon space capabilities for its sustainment.[4] Indeed, the ability for the United States to secure its interests in the Information Age rests largely in its ability to secure its access to space. At the same time, the number of space-faring nations has increased dramatically, generating new dynamics in the compulsory pursuit of national interests through space. In response, US policymakers and strategists correctly categorize the space domain as progressively *contested*, *congested*, and *competitive* and advocate the renewed importance of assuring US access amidst the changes.[5] Nevertheless, while emerging policies, reports, and operational plans recognize new challenges to operating in space, only disparate pockets of strategic, operational and tactical adjustments ever occur, none of which are compelled by a unifying strategy. Thus, a second problem set emerges:

- **Problem Set #2:** *The US military space infrastructure is not postured to ensure freedom of access, maneuver, or exploitation of space in a contested environment, thereby inhibiting the attainment of space control, information control, and, ultimately, national security in the twenty-first century.*

Synthesis of the Problem Sets and Resultant Thesis

The stage is set for formulating a strategic approach to future warfare that assimilates issues with joint warfare and space operations in the Information Age. The combination of stagnant, monolithic paradigms in space and an ever-expanding global information network has generated two interrelated security dilemmas that can only be reconciled together. A unifying solution emerges: *the United States should establish a comprehensive information control strategy designed to identify and secure access to the information environments that enable its desired way of warfare*. An overarching information control strategy, above and beyond theater campaigns, assumes preeminence in the new paradigm of force projection and application.

By extension, US space policy, strategy, and DOTMLPF—currently lacking in clarity and capacity—should develop under the greater umbrella of an information control strategy. This association reveals one critical, and yet often overlooked, attribute

[4] William E. Burrows, *This New Ocean: The Story of the First Space Age*, (New York, NY: The Modern Library, 1998), 611.
[5] US Department of Defense, *National Security Space Strategy* (Washington, DC: Office of the Secretary of Defense, 2011), 1-2.

of military space operations: space-based capabilities are intrinsically informational. Indeed, the dawn of the Space Age, the apex of the Industrial Age, actually represented the genesis of the Information Age, as space-based systems introduced the world to the notion of global and near instantaneous communications. Today, global space infrastructures—along with their cyberspace counterparts—constitute the backbone of modern information environments. In this regard, placing an information control strategy at the forefront creates a forcing function for the purposeful integration of space and cyberspace operations and establishes a strategic imperative for unified information control efforts *across the entire joint force*. Thus, space and cyberspace control strategies serve as requisite elements of an information control strategy and involve the mutual pursuit of controlling access to their respective domains. To this end, *the United States must adopt a space control strategy to secure freedom of access, maneuverability, and exploitation of space-based capabilities in support of an overarching information control strategy*. Collectively, the establishment of a prioritized information control strategy and its subordinate space and cyberspace control strategies describe a new paradigm—and a new way of warfare—for the twenty-first century.

Roadmap and Methodology

The framework explores the definition and impetus for information control as a national and joint warfighting objective and provides a general approach for setting the necessary conditions for its attainment. To this end, the paper is divided into two parts, congruent with the two problem sets explained above. The first part (Chapters 1 through 3) examines foundational concepts of strategy, C2, information, and information control en route to establishing a theoretical model for Information Age warfare. Part two (Chapters 4 and 5) builds on the framework and thoroughly examines the US Defense Department's space infrastructure as both a relic of the Industrial Age and an inadvertent arbiter of modern warfare. In this sense, the US military space program serves as both an exemplar of joint warfighting shortfalls and a notional model for transformation.

Chapters 1 and 2 build a framework for the role of information in warfare and how these realities manifest themselves in the Information Age. Specifically, Chapter 1 analyzes classical and contemporary military theorists such as Sun Tzu, Carl von

Clausewitz, Helmuth Graf von Moltke, B.H. Liddell Hart, J.F.C. Fuller, John Boyd, Martin van Creveld, and John Warden III to highlight the enduring roles of strategy, decision-making, and information in war. Within this context, historical relationships between information technology, force projection and employment, and C2 are inspected. In so doing, a baseline is set for understanding lasting qualities of war and their relevance in the Information Age. Chapter 2 carries this notion further by comparing specific Industrial and Information Age precepts—better described as kindred *paradigms*—and exploring information's evolving role in military operations across the periods. The intent is to provide a narrative that explains the origins and shortfalls of current mindsets driving joint operations. In the final section, information environments are identified and defined as *infospheres*, consisting of physical and information dimensions formed by space and cyberspace infrastructures. Global infospheres are considered unique artifacts of the Information Age and are thus used as a reference point to devise a new model of warfare. The identification and protection of infospheres are considered the central elements of an information control strategy.

Chapter 3 moves from theory to application by explaining how joint planning and operations may function after applying the theoretical propositions outlined above. Joint publications and planning concepts such as operational design provide currency and relevancy to the framework. The chapter unveils shortfalls in current joint planning assumptions and processes and offers a new paradigm for warfare in the Information Age, establishing revised definitions of *information control* and *information superiority*. Chapter 3 concludes by suggesting that joint force deficiencies—relative to the proposed warfighting concept—are reflected in the military space culture, paving the way for investigating the US space infrastructure and establishing a new space control methodology from the information control model.

Chapter 4 serves as a stage setter for part two by discussing the US military space program's history and its influence on the current paradigm that shapes not only its culture but also national and joint warfighting policies and strategies. Chapter 4 concludes with conceptual and actual diagnoses of emergent counterspace threats and their impact on national security considerations in space. Ultimately, the intent is to explain why the US space infrastructure is not designed to support the information

control construct developed in the first three chapters. The chapter closes by posing a series of transitional—yet profoundly significant—questions regarding space control and space superiority: How does a military know that it holds space control or superiority? How does it know when space control or superiority is lost? What actions are required to achieve control and/or superiority in space? What agency is responsible for obtaining and assessing space control? And finally, what is the proper role of the military in space?

Chapter 5 synthesizes parts one and two using the contextual backdrop provided by Chapter 4. The chapter is divided into two portions. The first portion creates a notional methodology for space control based on the theoretical framework created in part one. The second portion reveals that extant space strategies and policies are inappropriate for the proposed model, as current space DOTMLPF fall short of supporting a comprehensive space control strategy and in some cases inhibit its realization. Each aspect of the USAF's space DOTMLPF is scrutinized under the framework established in Chapters 1 through 3 and the space control method laid out in the chapter's first portion, denoting opportunities for transformation where applicable.

The concept of information superiority is not new, nor is the realization that the Information Age presents impending challenges to national security. Furthermore, the call for a space control strategy dates back several decades in the US military but is routinely stifled by political sentiments and the lack of a convincing imperative. Indeed, multiple doctrinal and academic publications address various aspects of the topics introduced above. However, the proposal for a new way of warfare that prioritizes information control at the strategic level and associates space operations and space control within an integrated information control strategy offers a unique perspective on warfighting in the twenty-first century. So too is the recognition that adopting a comprehensive information control strategy is an essential first step in transforming an Industrial Age military into an Information Age force. America's ability to exploit sophisticated information technologies and advance its interests in a semi-permissive environment is quickly coming to an end. More than ever before, the United States must consider its options for shaping the character of war in its favor, and the theoretical framework constructed in the ensuing analysis provides a guideline for change.

Chapter 1

Strategy, Decision-Making, and Information in War

What has been will be again, what has been done will be done again. There is nothing new under the sun.

- Ecclesiastes 1:9

The interplay between continuities and disruptions will demand a Joint Force that can see both what has changed and what endures.

- Joint Operating Environment, 2010

Conflict and human nature are inexorably linked. To understand conflict—up to and including war—is to understand the motivations behind human behavior, and conflict's perpetual existence is reinforced through the annals of history. Indeed, great importance is attributed to the writings of Thucydides, Sun Tzu, and other classical historians and theorists not only because of their keen insights, but also because of the profound connection made with humans living 2,500 years ago: there is direct applicability to current predicaments despite the progression of time. Across that span of time, literature on warfare and human nature abounds, each thesis attempting to explain the world as it is, or as it could be, all in human terms. However, in an age frequently described as dynamic and ever changing (with the rate of change considered by some as the greatest challenge humans face), grounding oneself to enduring aspects of the human experience provides a way of characterizing, managing, and addressing seemingly chaotic events, including war.

The analysis thus begins with an examination of war's enduring qualities. The first chapter's purpose is to establish a theoretical foundation of war to properly assess its characteristics in the Information Age. Specifically, the opening analysis seeks to find continuity by revealing the timeless relationship between strategy, decision-making, and information in warfare. This common frame of reference may alleviate some of the underlying concerns (or fears) based on growing uncertainties induced by the perceived complexities associated with Information Age warfare. More importantly, the theoretical foundation serves as a point of reference for assessing whether the US military is postured to preserve its desired way of warfare in the twenty-first century.

To this end, war's enduring qualities and evolving characteristics are examined in detail. First, war's nature is revealed as an extension of human nature and propelled by the tension of rational and emotive impulses. Subsequently, the essence of strategy is described, establishing context for exploring the timeless relationship between decision-making and information. In this sense, strategy demonstrates its utility by providing avenues for gaining an advantage over an opponent and securing a desired amount of situational control or influence. Strategy development and implementation drive decisions, which require a baseline set of information capable of distinguishing options from which to decide and act, regardless of how the war is waged. The chapter then transitions to examining war's evolving character and information technology's influence on its conduct. In particular, information technology's effect on force projection, force employment, and command and control (C2) throughout history is assessed, establishing a conceptual bridge for investigating information's role in modern warfare.

Description of Terms

Before proceeding, a brief description of key terms introduced in this chapter is warranted. At the most basic level, *data* includes observations and signals collected by various sensors (human and/or mechanical) with "distinct units or values."[1] Data by itself or without reference to a broader purpose has no intrinsic significance. The term *information* carries a wide range of connotations, but is consistently described as data interpreted within a specific context "to inform or provide meaning for action."[2] In other words, data assumes its relevance as information when sought and/or employed by the receiver, human or machine, to decide and act according to situational requirements. Of note, the circumstantial relevance associated with information (processed data) unveils an important reality detailed in subsequent chapters.[3] Together, data and information constitute the *organic essentials* of decision-making and action—the focus of the analysis—rather than the content of the messages transmitted or received.

---

[1] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms,* 8 November 2010 (amended through 15 December 2014), 61.
[2] JP 3-13, *Information Operations*, 20 November 2014, I-3.
[3] Greater emphasis is placed on the physical systems employed to collect and disseminate information and the prioritized information requirements placed upon the collection systems themselves.

Operational concepts such as *information control*, *information superiority*, and *information warfare*, discussed in detail later, involve relative conditions pertaining to one's situation (strategy) and the act of securing those conditions. Information control indicates an ability to collect, process, and disseminate requisite data in both optimal and degraded environments. Comparatively, information superiority applies to one's level of information control in relation to an adversary's—the resultant advantage gained by securing a higher level of information control relative to the opponent.[4] Information warfare consists of offensive and defensive actions taken across multiple domains to secure information control and information superiority.

As the analysis unfolds, refined descriptions of information control and information superiority will emerge under a new paradigm of war. The overall intent is to explore how the joint force can establish conditions to ultimately enable the attainment of information control and its significance with regard to strategy. At present, with preliminary descriptions of data, information, information control, and information superiority in place, attention now turns to the timeless phenomena of war and conflict.

War's Enduring Nature

Humans, the initiators and executors of war, remain at the heart of war's nature. Therefore, a discussion of war's nature cannot commence without first examining enduring qualities of humanity. Humans are fallible and finite beings.[5] This inherent condition is characterized by intense self-centeredness, a consuming fear of the unknown, and a subsequent desire to influence future outcomes favorable to self-interests. In other words, humans seek stability in an otherwise chaotic world. Indeed, Kenneth Waltz revealed that humans try to understand their world from "the desire to control, or at least to know if control is possible, rather than merely to predict" events.[6] In most telling fashion, the unquenchable demand for and existence of *theoretical* frameworks to explain the world are testaments to the pervasive limitations of the human condition. As a result,

[4] JP 1-02, 119.
[5] Terry Nardin and David R. Mapel, eds., *Traditions of International Ethics*, (Cambridge: Cambridge University Press, 1992), 86.
[6] Kenneth N. Waltz, *Theory of International Politics*, (Long Grove, IL: Waveland Press, Inc., 1979), 6.

humans place high value on sources of power that enable them to achieve personal interests and shape their destinies amidst their frailties.[7]

The realities of the human condition and its resultant nature explain the existence and characteristics of competition that leads to conflict. When humans fight (physically or verbally), they are ultimately trying to gain the advantage over their adversaries by creating opportunities to shape or exert some level of control over the outcome, commensurate with interests, values, and priorities. To accomplish this, humans must understand the political, strategic, operational, and tactical environments within which they choose to decide and act. These environments are shaped by many factors, not the least of which is other actors who constantly pursue their own interests while assessing their situation relative to others. When these interests, values, and priorities collide with sufficient magnitude, conflict ensues, drawing uncertainty with it. Humans engage one another with the fundamental intent of positioning themselves and their resources in such a way as to gain an advantage relative to others and control events in ways that meet their objectives.[8]

Expanding this construct to international relations provides a basis for translating generic forms of human conflict to war, an institution of sanctioned violence between collective groups. Humanity's egoistical nature exists alongside an innate desire for social interaction and identity, leading to a natural formation of group structures. Today, these groupings take many forms, culminating in the state, the highest social collective and the primary unit in international relations. By legitimizing the group's (i.e., state's) sovereignty, humans cede a portion of their individual interests to the collective with the acceptance that group interests will subsume them.[9] In so doing, humans impart the responsibility of securing interests to the group, invariably generating friction points within the larger social system. In relation to modern societies, Waltz adeptly explains "the actions of states" are better qualified as "men acting for states," and these actions "make up the substance of international relations."[10] Consequently, "the national interest

---

[7] Nardin and Mapel, 87.
[8] Not all analysts agree with the model of human nature and the inevitability of war presented here. For a counterpoint to this view, reference John Horgan, *The End of War*, (San Francisco, CA: McSweeney's, 2014), 24.
[9] Nardin and Mapel, 93.
[10] Kenneth N. Waltz, *Man, the State, and War*, (New York, NY: Columbia University Press, 1954), 122.

. . . is likely to be pursued in an essentially egoistic way in respect to other states."[11] By transposing human nature into the behavior of states, one can expect states to operate with the same fears, values, and priorities that circumscribe human beings. Therefore, social systems involve collective groups that seek to secure their self-interests and influence future outcomes, resulting in a competitive environment that prompts them to increase their power to mitigate threats posed by others. In today's strategic environment, national interests are pursued in identical terms within the international system. The resulting clash of state (and non-state) actors represents an analytical framework for war.

In reviewing historical trends of war, several prominent observations emerge regarding its nature, separated in time by millennia and geographical locations by thousands of miles. First, in the opening line of his seminal work *The Art of War*, Sun Tzu proclaims, "War is a matter of vital importance to the State; the province of life or death; the road to survival or ruin . . . war is a grave matter."[12] Similarly, two thousand years later, Carl von Clausewitz described war as "a serious means to a serious end" and "such a dangerous business" that "it would be futile—even wrong—to try and shut one's eyes to what war really is from sheer distress at its brutality."[13] This ferocity stems from human behavior in response to self-generated motivations and the fears associated with a loss of perceived control or influence—or the pursuit of self-gratification. As though analyzing the same evidentiary base as Sun Tzu and Clausewitz, Thucydides adeptly surmised a timeless triad of human motivations for conflict, all self-fulfilling: fear, honor, and interests.[14] War, then, develops from and incorporates an amalgamation of intertwined factors set in motion by what Clausewitz termed *hostile intentions* aimed at those whose desires impinge on one's own. Hostile intentions, according to Clausewitz, represent war's "universal element."[15]

---

[11] Nardin and Mapel, 93.
[12] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (London: Oxford University Press, 1963), 63.
[13] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75-76.
[14] Thucydides, Robert B. Strassler, Richard Crawley, and Victor Davis Hanson, *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War; with Maps, Annotations, Appendices, and Encyclopedic Index*, A newly rev. ed. of the Richard Crawley trans., (New York, NY: Simon and Schuster, 1998), 43.
[15] Clausewitz, 76.

The reality of human nature and its willingness to employ violence against others in the preservation of self—during and after conflict—within any given social structure provides a broader context for war's ultimate purpose and conduct. Clausewitz's oft-cited description sets the stage for further analysis. War, "the collision of two living forces," amounts to "an act of force to compel our enemy to do our will."[16] War thus allows for the transfer of human motivations to hostile intentions with the aim of suppressing enemy opposition and reducing, or eliminating, his power to resist. On the international scene, war manifests itself from the political objectives set forth by the governing body and is directed at compelling state and non-state actors alike (albeit in potentially different ways) and setting post-conflict conditions that create an environment conducive for securing future goals.

It is at this point where the true contention in war lies. As Clausewitz's theory suggests, the impact of two living entities striving to impose their respective will on the other creates an incentive to overcome the opponent's ability and/or desire to wage war. As such, one "must either make [the enemy] literally defenseless or at least put him in a position that makes this danger possible," thereby overcoming his opposition by disarming him, permanently or provisionally. The very requirement to engage the enemy and deny him his objectives (while achieving one's own) implies an initial condition where neither side boasts control of the other, creating the pathway for conflict resolution as each side vies for power and influence to ultimately impose its will.[17] Indeed, strategist and theorist J.C. Wylie concluded, "the aim of war is some measure of control over the enemy," constituting the central tension in conflict.[18] The consuming effort to exert control over another living force unleashes war's brutality and drives the belligerents to devise methods that minimize their own suffering (and uncertainty) and maximize the adversary's. Such is the essence of strategy.

War as an institution and war theory provide tangible and conceptual approaches to stabilizing an otherwise chaotic endeavor, allowing humans to employ violence as an instrument for shaping events and reinstating a level of certainty in outcomes. In this

---

[16] Clausewitz, 75, 77.
[17] Clausewitz, 77. "So long as I have not overthrown my opponent I am bound to fear he may overthrow me. Thus I am not in control: he dictates to me as much as I dictate to him."
[18] J.C. Wylie, *Military Strategy: A General Theory of Power Control*, (Annapolis, MD: Naval Institute Press, 1967), 66.

light, strategy serves as a methodology to gain the advantage necessary for political control and influence during and after conflict. It is through strategy development, execution, and assessment that information's role in war emerges. The following discussion thus turns to the indisputable link between strategy, decision-making, and information when defining and attaining success in war.

Foundations of Victory: Strategy, Decision-Making, and Information

Strategy embodies such a sweeping array of considerations that no universally accepted definition exists. Indeed, throughout history, hundreds of theorists, academics, and practitioners have derived an equal number of conclusions on strategy's essence and purpose.[19] The lack of an established frame of reference notwithstanding, the previous examination of war's nature and its direct relationship to human tendencies provides a useful baseline for formulating a broad description of the term.

Human nature places high value in both certainty and control in its pursuit of self-interests. In this endeavor, and due to their social interactions, humans inevitably infringe upon others' attempts at building certainty and control. As humans navigate their way through life, personally and collectively, they realize circumstances do not naturally generate favorable conditions for their desires. Thus, an approach is necessary to prioritize needs, allocate resources, assess limitations, threats, and risks, and manipulate conditions that subsequently enable the attainment of objectives. Strategy incorporates both a process and product that strives to shape the environments within which humans operate. These environments invariably include opposing actors—and their strategies—attempting to accomplish the same.

From a state's perspective, two forms of strategy typically exist: grand strategy and military strategy. Grand strategy involves a broader range of objectives and encompasses a long view of conditions, before, during, and after war. In effect, grand strategy sets the framework from which all other subordinate strategies develop and support. As B.H. Liddell Hart observes, "The object in war is to attain a better peace—even if only from your point of view…. If you concentrate exclusively on victory, with

[19] Colin S. Gray, *Modern Strategy*, (New York, NY: Oxford University Press, 1999).

no thought for the after-effect, you may be too exhausted to profit by the peace."[20] Therefore, the terms of peace and the conditions under which peace thrives constitute the primary contribution of grand strategy. To this end, grand strategy prioritizes and mobilizes a state's combined resources. Military strategy, in turn, derives its purpose from grand strategy and complements the overall effort, focusing on the projection and application of force to set favorable conditions set forth by grand strategy.

For the purposes of analysis, one other distinct difference separates military strategy from grand strategy and sets the stage for understanding the role of information in war. Grand strategy entails far-reaching goals that exist both independent of and in reference to the current and/or anticipated geopolitical landscape. Military strategy, on the other hand, sets its course based on assessed threats to grand strategy's schemes and is thus built to counter specific, or emerging, adversaries. Consequently, while grand strategy articulates the underlying stimuli for conflict, military strategy represents the volatile point of contact between opposing forces. Sun Tzu's profound assertion carries the thrust of this human endeavor: "What is of supreme importance in war is to attack the enemy's strategy."[21] The role of information in war now crystalizes within the context of strategic advantage.

Undermining the enemy's military strategy (referred to as strategy henceforth) presents the mechanism by which one side can gain the advantage over another and impose its will. Congruent with Clausewitz's illustration of two forces colliding, Liddell Hart indicates strategy's aim "*is to diminish the possibility of resistance*" (emphasis in original).[22] Before conflict begins, however, neither side boasts sufficient control over the other (otherwise war would serve no practical purpose). It is for this reason that one's strategy must focus on overcoming the adversary's strategy, requiring calculated applications of force relative to the *specific* adversary. Thus, *strategy is meaningless without an understanding of the character of resistance faced*.

The information requirements levied through strategy development represent enduring aspects of war. In seeking to "know the enemy," strategists require information on the enemy's overall intent; "principle actors and their interrelationships; cultural

[20] B.H. Liddell Hart, *Strategy*, 2nd rev. ed. 1967 (Reprint: New York, NY: Penguin, 1991), 353.
[21] Sun Tzu, 77.
[22] Liddell Hart, 323.

relationships; historical context; physical geography; instruments of power; elements of power; and political, military, economic, social, information, and infrastructure (PMESII) elements."[23] Just as importantly, and increasingly challenging, is the demand to "know yourself," or the location, disposition, posture, capabilities, limitations, susceptibilities, et al. of one's own forces. In relating the enemy's strategy to one's own, strategists can then identify vulnerabilities and formulate an exploitation strategy to eventually gain strategic leverage and exert control over the opponent. Sun Tzu once again offers a clear summation when he advises, "Determine the enemy's plans and you will know which strategy will be successful and which will not."[24]

Strategy development functions to orchestrate the sequential and/or cumulative actions (and reactions) of all available resources to achieve the necessary advantage across the spectrum of conflict. However, as strategy transitions from development to implementation, the physical and psychological concussions resulting from the clash of two living entities generates the detrimental effects of *fog* and *friction* characterized in Clausewitz's theory. Although resolved somewhat differently, Sun Tzu, Clausewitz, Liddell Hart, and J.F.C. Fuller conclude that uncertainty in war continually tears at the fabric of strategy. Clausewitz recognizes friction as an unavoidable reality of war, emanating from unforeseen circumstances and requiring the superior intellect of a commander to sift through the quagmire and extract ground truth from obfuscation. While Sun Tzu, Liddell Hart, and Fuller recognize the intangible qualities of a commander's mind, they extend their theoretical approach to finding ways that minimize one's own friction and maximize the adversary's, achieved through the application of surprise and deception.[25] Combining these approaches offers a critical correlation between strategy and decision-making.

The cognition and resultant interpretation of information exceeds the scope of this analysis, but the information requirements (i.e., the organic essentials) set forth by decision-makers represent the cornerstone of the comprehensive thesis. In this sense, the commander's role in strategy development and implementation cannot be overstated.

---

[23] Sun Tzu, 84.; Jeffrey M. Reilly, *Operational Design: Distilling Clarity from Complexity for Decisive Action* (Maxwell AFB, AL: Air University Press, 2012), 6.
[24] Sun Tzu, 100.
[25] Sun Tzu, 66.; Liddell Hart, 323.; J.F.C. Fuller, *The Foundations of the Science of War*, (London: Hutchinson and Company, 1926), 213, 224, 273.

Indeed, the complexities of war are such that "a competitive advantage derives from a synthesis of a critical mass of relative advantages in several arenas: information, knowledge, understanding, [and] decision-making."[26] As strategy coordinates actions across a range of mission areas, commanders provide guidance through their intent. Successful commanders in history such as Frederick the Great, Napoleon Bonaparte, and Helmuth Graf von Moltke each articulated an overarching vision that bound their respective forces under a unifying campaign, optimizing unit cohesion and effectiveness on the battlefield. The realm of strategy, then, also involves translating a commander's intent into action and therefore requires routine interaction with the central authority.[27] To this end, strategy anticipates, identifies, and incorporates decision-making opportunities for the commander, facilitating a more effective and unified response to the inevitable uncertainties that spring from the throes of combat. Because strategy exists to generate a level of certainty to help shape conditions commensurate with one's intent, informed decision-making "determines who has the initiative and ultimately who wins."[28]

The confluence of strategy development, strategy implementation, resultant friction, and the facilitating of decision-making reveal the eternal role of information in war. Strategy fundamentally exists to generate leverage, gain control, and impose one's will over another. However, when opposing forces interact violently, it sparks a series of unanticipated events that increase friction in the form of uncertainty, fear, and surprise. This uncertainly demands keen intellect to decipher reality and also offers a gateway for undermining an adversary's strategy by instilling an unacceptable amount of friction into his perceptions and processes. Strategy, therefore, also serves to add clarity by augmenting decisions based on commander's intent and the enemy's actions. For its part, decision-making requires not only a certain amount of information but also particular types, depending on the circumstances. As decision points emerge (planned or dynamic), they are fed by a series of predetermined and ad hoc information requirements. Accordingly, strategy development provides a systematic approach for identifying and

[26] David S. Alberts, John J. Garstka, Richard E. Hayes, and David A. Signori, *Understanding Information Age Warfare*, (Washington, DC: DoD Command and Control Research Program), 41.
[27] Chapter 3 covers this theme in greater detail.
[28] Reilly, 1.

prioritizing information requirements corresponding to decision makers' needs in anticipation of the friction that ensues upon execution.

In the pursuit of gaining an advantage, sound strategy instills a level of certainty in one's situation to rebalance war's disruptive effects while elevating the adversary's uncertainty.[29] Opposing strategies therefore set operational parameters for information control and information superiority. Informational needs fluctuate by strategy and opponent, forming what some consider an "asymmetrical" comparison. In this regard, "what will matter is which force does a better job satisfying their respective information needs."[30] Thus, *information by itself is useless, and its utility is determined through strategy and the decisions made during its creation, execution, and assessment*. How information requirements are met and the types of decisions they support vary in time and space and represent the shifting character of war. Nevertheless, the connection between information, decision-making, strategy, and victory comprises an enduring relationship in war, and one that sets the framework for the remainder of the thesis. In the end, any advantage gained by counterbalancing friction in war is strengthened by information control.

Gaining the Advantage Through Information Warfare: A Brief Synopsis

Prior to examining war's nature through its evolving character, a conceptual illustration of information warfare for the attainment of information control and superiority provides a backdrop for assessing the implications of the Information Age in subsequent chapters. The basis of information warfare, as an operational approach, subsists within the synthesis of modern and historical thought.

As a counter to ambiguity, Clausewitz purported the intangible advantage of *military genius*, which ultimately enables great commanders to make shrewd decisions despite the confusion surrounding war. Certainly, the flow of new information during war "continually impinge[s] on our decisions, and our mind must be permanently armed .

---

[29] See Alberts et al., 54: "The concept of an information advantage is not new. Commanders have always sought—and sometimes gained—a decisive information advantage over their adversaries. Indeed surprise, one of the immutable principles of war, can be viewed as a type of information advantage…."
[30] Alberts et al., 55.

. . to deal with [it]," demanding "a skilled intelligence to scent out the truth."[31] Similarly, Sun Tzu asserted that the "intellectual faculty of man [was] decisive in war, and that if [it] were properly applied war could be waged with certain success."[32] He continued on to say that a prudent commander "is able to recognize changing circumstances and to act expediently."[33] Thus, Clausewitz' and Sun Tzu's recognition of war's uncertainty and detailed assessments of military genius all emerged within the confines of its persistent nature, examined earlier.

This theoretical depiction establishes a requisite foundation for formulating how strategy can persist in an ambiguous environment. Colonel John Boyd's well-documented model for decision-making, the OODA loop (observe, orient, decide, act), sets the framework for processing information in suboptimal situations. Boyd's model captures war's essence and highlights decision-making as the cornerstone of victory in combat. As such, Boyd saw warfare through the lenses of time and mind rather than through the physical dimension. Boyd understood that the military objective is "to break the spirit and will of the enemy command by creating surprising and dangerous operational or strategic situations."[34] To achieve this effect, Boyd sought to overwhelm his adversary by reducing the time available for detecting, interpreting, and responding to threatening stimuli (genuine and assumed) by rapidly conducting multiple, varied maneuvers and controlling the information presented, thereby influencing his adversary's decision-making capacity. Consequently, by denying the ability to decipher the surrounding environment, Boyd believed humans would reach a point of "paralyzing panic," negating their ability and/or willingness to resist.[35] Liddell Hart described this phenomenon as the "dislocation of the enemy's psychological and physical balance" in what he considers a "vital prelude to a successful attempt at his overthrow."[36]

Thus, he who makes the best and quickest decisions—*in relation to his adversary*—creates conditions for success. Conversely, he who is unable to make timely and accurate decisions (due to strategic paralysis imposed through Boyd's model), again,

---

[31] Clausewitz, 102.
[32] Sun Tzu, 39.
[33] Sun Tzu, 65.
[34] Quoted in Major David S. Fadok, *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis*, (Maxwell AFB, AL: Air University Press, 1994), 14.
[35] Quoted in Fadok, 15.
[36] Liddell Hart, 6.

relative to his adversary, cannot achieve success. Therefore, one's primary objective in securing victory must be to make accurate decisions faster than the adversary, *which first requires safeguarding one's own decision cycle (facilitated through information processing), then degrading or disrupting the adversary's decision cycle, and/or a combination of both, in the fulfillment of one's strategy.*

According to Boyd's model, proper *orientation* plays a pivotal role in the decision-making process, and by extension, a critical aspect in gaining the advantage over an opponent.[37] Two factors enable effective orientation, one at variance with personal tendencies and the other controllable. The first enabler involves the decision maker's genius, as previously described by Clausewitz and Sun Tzu. This aspect is directly dependent upon the decision-maker's personal capabilities and is empowered through the second factor: that of timely, accurate, and pertinent information, codified through Boyd's *Observe* step and derived through strategy development. Thus, to affect the adversary's ability to *Orient*—and therefore disrupt his decision-making potential—one should seek to target his ability to *Observe* while simultaneously protecting one's own methods of observation. This approach, a basis for information warfare and a function of war's nature, creates an operational imperative for gaining information control and, if needed, information superiority—in any conflict.[38]

War's Evolving Character

The enduring qualities of strategy, decision-making, and information manifest themselves through war's character, distinct from war's nature in that it describes *how* wars are fought rather than *why*. Changes and differences in technology, economic structures, social constructs, political structures, geography, objectives, and threats influence the conduct of war. How strategy, decision-making, and information coalesce constitutes war's character, but the fundamental relationships between the three elements remain intact. In determining how this relationship translates itself to the conduct of war,

[37] Fadok, 16.
[38] Of note, Boyd's theories encompass much more than his iconic OODA loop. Nevertheless, many documents highlight the OODA loop as a model of simplicity, perhaps overemphasizing the importance of speed in decision-making. Indeed, Boyd developed a comprehensive—if not dynamic—theoretical framework aimed at promoting a new way of thinking rather than creating a prescriptive approach to warfare. For further details, reference Frans P.B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd*, (London: Routledge, 2007), 1-8.

evolving technological advancements in information collection and dissemination and their relationship to force projection and employment requirements and command and control methods and structures are now examined. It is through war's character, not its nature, where strategists ultimately find the Information Age's true impression on war.

Information Technology and Warfare

Joint publications and academic analyses categorize information technologies in various ways, but all agree in the standard functions of collection, processing, and dissemination.[39] Processing, however, involves human and/or machine interpretation of data, which induces a higher level of subjectivity than desired for examining information's role in war. As a result, collection and dissemination technologies represent the basic functions of information networks with objective qualities and therefore warrant the focus of the analysis.

While related, and interdependent in terms of providing any operational utility, collection and dissemination comprise fundamentally different purposes and are not necessarily bound by one particular form of the other. Indeed, technological and operational developments in information collection and dissemination remained largely disjointed until the first half of the twentieth century. Collection, at its core, incorporates two essential aspects. The first aspect involves the ability to access required information. Access can involve physical locations such as high ground, air, space, underwater, and fiber optic cables, and virtual locations such as cyberspace networks and the radio frequency (RF) spectrum (frequency and bandwidth). The second aspect of collection involves the method of collection; that is, the active or passive collector of data, or the sensor—what it can detect, and how it detects it. The human body (eye, nose, hear, tongue, nerve endings), telescopes (lenses), radar, and multi-spectral imagers all constitute various collection methods. Of note, many sensors function as an extension or enhancement of basic human perceptions, particularly vision and sound, but others, such as radar and multi-spectral imagers, are capable of collecting a substantially wider range of inputs by functioning across the entire electromagnetic spectrum (EMS). Access requirements and collection methodology are both dictated by mission needs. Collection

---

[39] JP 3-13, *Information Operations*, 20 Nov 14.; Alberts et al., 40.

technologies, then, are characterized and constrained by their ability to access areas of interest and their sensory capabilities.

Information dissemination technologies include a different subset of capabilities, many of which originally did not relate directly to information distribution. Like the collection function, dissemination technologies carry two prominent features: speed and reach. As distribution capabilities and requirements increased, so too did their ability to traverse greater distances in shorter amounts of time. Initially, information distribution was made possible through methods of transportation and sound manipulation (e.g., speaking and drumming).[40] The foot, horse, and railroad all connote physical methods for maneuvering people and goods, yet they simultaneously served as information dissemination technologies by supporting the flow of verbal communication. Eventually, and in similar fashion to advancements in collection technologies, information dissemination evolved beyond physical boundaries—and simple augmentation of human abilities—to include electronic distribution methods capable of transmitting information previously inaccessible to humans across the globe and at the speed of light. Over time, "military communications progressed from runners to smoke signals and signal flags to telegraph to radio to telephone to video teleconferencing to a fully functioning collaborative work environment."[41]

In tandem, collection (access and method) and dissemination (speed and reach) technologies encompass the central elements of information flow (see Figure 1). Neither capability provides standalone utility: to acquire requisite information for strategy implementation in the way of decision-making and action, one needs the proper coordination of collection and dissemination capabilities. Needless to say, even in the most permissive of environments, the lack of coordination or integration of these technologies may preclude the attainment of vital information for processing. Moreover, any degradation to one or both functions could instigate severe consequences. Thus, *proper planning, coordination, integration, prioritization, and protection of information collection and dissemination capabilities constitute fundamental considerations for operations in war*.

---

[40] James Gleick, *The Information: A History, A Theory, A Flood*, (New York, NY: Vintage Books, 2011), 13.
[41] Alberts et al., 47.

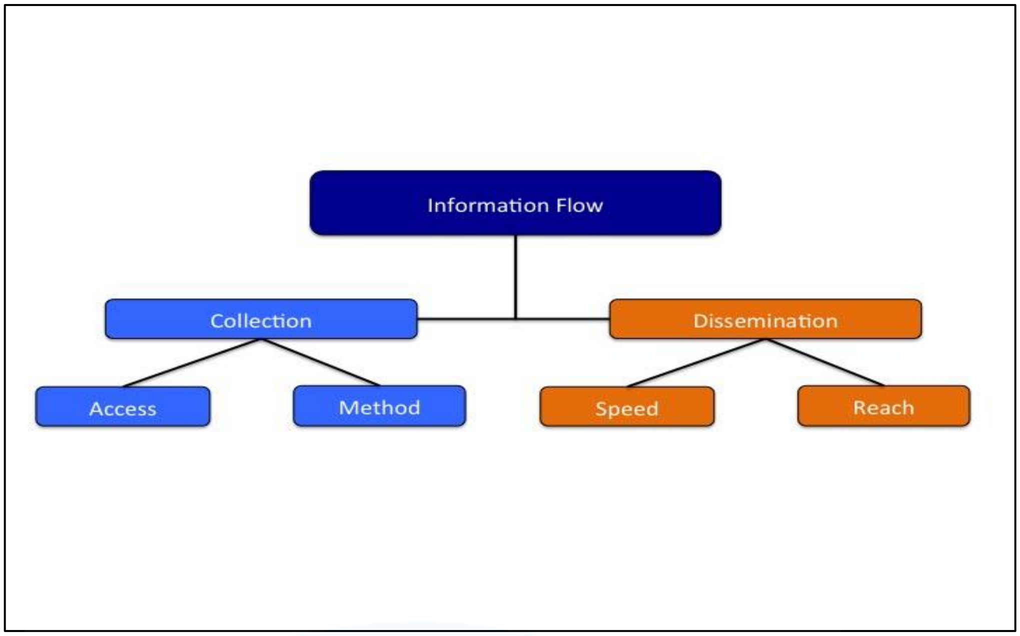

Figure 1: Basic Elements of Information Flow
Source: Author's Original Work

Nevertheless, available technology limited the relevance and enforcement of this primitive concept prior to the twentieth century. Four historical examples illustrate how information collection and dissemination processes developed over time, and set the stage for further discussions on Information Age properties. The first example covers warfare from antiquity until the mid-1800s. From a collection standpoint, little advancement was made beyond human senses. Perhaps the most notable collection technology employed during the period was light refraction in the form of convex lenses and telescopes. From an access standpoint, commanders and scouts would seek the high ground (or cover) to purview the landscape and track enemy movements. Information dissemination occurred by word of mouth (or hand-written notes) and was augmented by the employment of messengers, various signals, and/or horses, as indicated above. By the mid-1800s, the emergence of the railroad and telegraph reshaped the way war was perceived, planned, and fought. However, in both cases, these methods of dissemination were not bolstered by any true advancement in collection capabilities. In essence, the railroad and telegraph

allowed for a greater dispersal of information that was still collected through traditional means.[42]

At the turn of the twentieth century, a single technical achievement significantly transformed information collection options in terms of access: the airplane. When the concept of air warfare gradually crept into the minds of policy makers by 1899, attempts were made to regulate, and even restrict, the use of aircraft for offensive purposes.[43] After the airplane materialized in national inventories, several experiments commenced to determine its value as an observation tool. Observation balloons had already entered the service decades prior, but the advent of the airplane offered a means for rapid mobility and, ultimately, information collection. As late as the First World War, artillery represented the most crucial weapon of any army and advancements in range and accuracy created situations in which "the gunners in World War I batteries almost never saw their targets."[44] Thus, observation balloons were employed to identify enemy locations based on their advantageous access points in the sky—the balloons were essentially unmolested.

As the airplane took flight in combat, an early form of information warfare commenced, and a clear example of war's nature transpired. Information gleaned from observation balloons (and airplanes) fed into a dynamic loop indicative of the modern day strike process known as F2T2EA (find, fix, track, target, execute, and assess). Artillery batteries could effectively employ their long-range capability without direct engagement, gaining a distinct advantage on the battlefield. In an attempt to counter that advantage, made possible through information collection and dissemination, militaries used airplanes to destroy the defenseless observation balloons and acquire intelligence in the process. Conversely, realizing the consequences of lost information, enemy forces devised ways of neutralizing the new threat from the air, and an escalatory conflict ensued as both sides sought control over the domain (*and thus controlled access to information collection platforms*). Although the airplane displaced the balloon as a

[42] The Union Army did conduct limited signals collection on Confederate telegraph transmissions during the American Civil War, denoting an early employment in electronic signals intelligence, or SIGINT. See Eliot A. Cohen, *Supreme Command: Soldiers, Statesmen, and Leadership in Wartime*, (New York, NY: Anchor Books, 2002), 28.
[43] Lee Kennett, *The First Air War: 1914-1918*, (New York, NY: The Free Press, 1991), 2.
[44] Kennett, 26.

primary observation platform, it only advanced information collection in terms of access. Binoculars and the human eye remained the dominant sensors for collection, and word of mouth, notes, and, later, radios served as dissemination options. Interestingly, what traditionally marks the advent of air warfare and air superiority serves best to illustrate information warfare conducted through the air medium.

The final two historical examples, covering World War II (WWII) and the Cold War, respectively, reveal a key transition in the relationship between information collection and dissemination capabilities and the overarching role information played in war and peace. By the time WWII ignited, air power had transitioned from a peripheral fascination to a central defense strategy for the United States and, to a lesser extent, Great Britain. Experiences in WWI and fears of a German air invasion had prompted Britain to invest its limited defense budget in air defense capabilities in the 1930s.[45] Failed experiments in sound-location technologies for aircraft detection led to the experimentation of radio waves for the same function. Previously tested for naval operations in the early 1930s, radar technology proved capable of detecting and locating aircraft and was incorporated into an elaborate air defense apparatus designed by Hugh Dowding. The architecture, coined the Dowding System, involved an intricate array of ground-based radars connected through a web of communication lines to dispersed air control facilities.[46] When the Luftwaffe finally took to the skies over England in 1940, Britain's air defenses exploited the blanket of invisible RF signals penetrating its airspace. Early warning of enemy location and direction proved invaluable against a superior air force, and, interestingly, the Luftwaffe never targeted the radar stations or communication nodes that fed the Dowding System—a gross oversight and a failure to appreciate the operational importance of information warfare. As an exemplar of information technology, the Dowding System was a complex and intricate communication network that fed timely, accurate, and pertinent information to decision-makers. Britain's entire air defense establishment—its doctrine, operations, training, etc.—modified itself based on the information the system provided; information (collected and disseminated) that could no longer be replicated by human abilities.

[45] Stephen Bungay, *The Most Dangerous Enemy: An Illustrated History of the Battle of Britain*, (Zenith Press), 42.
[46] Bungay, 46-47.

A final and enduring example of information technology in warfare comes from the Cold War epoch. The 1940s and 1950s saw the dawn of the nuclear age and threat of global annihilation. Warheads of inconceivable firepower were mated to delivery systems capable of penetrating the most advanced defense networks anywhere on the globe, ultimately reshaping perspectives on military strategy, deterrence, and associated intelligence collection requirements. By the late 1950s, the greatest risk to US national security and existence was perceived as a surprise nuclear attack from the Soviet Union. Consequently, President Eisenhower demanded timely, accurate, and persistent information on Soviet strategic capabilities. This fear intensified on August 26, 1957 when the Soviet Union conducted its first successful intercontinental ballistic missile (ICBM) test, sparking paranoia in the United States of a possible missile-gap.[47] In a dual effort to confirm ICBM inventories and ascertain resultant US defense budget requirements, Eisenhower stressed the need for intelligence collection over the Soviet mainland.[48] Information collection capabilities had already reached unprecedented levels; both in access and sensor technology, and dissemination technologies also surpassed any previous capabilities from WWII. However, preliminary intelligence collection operations required high altitude aircraft such as the U-2 to traverse Soviet (sovereign) airspace and collect images of nuclear activity prior to detection and/or engagement by Soviet air defenses. Additionally, the secret U-2 flights were invariably limited by fuel capacity, placing additional restrictions on the ability to acquire persistent intelligence. Early U-2 flights obtained imagery that suggested preliminary concerns over Soviet missile capabilities were possibly exaggerated, but Soviet air defense technologies were soon capable of detecting and engaging the U-2, resulting in the loss of U-2 aircraft and instigating political outcry from both sides.

The launch of *Sputnik* on October 4, 1957 changed everything. The space age sprang from the heels of the nuclear age and larger Industrial Age, consuming the breadth of resources and expertise available to Soviet and US defense industries. From a national perspective, the space infrastructure provided a profound increase in information

---

[47] Dino A. Brugioni, *Eyes in the Sky: Eisenhower, the CIA, and Cold War Aerial Espionage*, (Annapolis, MD: Naval Institute Press, 2010), 227-228.
[48] Walter A. McDougall, *The Heavens and the Earth: A Political History of the Space Age*, (Baltimore, MD: The Johns Hopkins University Press, 1985), 134.

collection and dissemination capabilities and requirements. The United States, politically hindered by the Soviet neutralization of its U-2 flights, pursued an alternative means for aerial espionage that eliminated the detriments inherent in air operations: namely infringement of sovereign airspace (drawing political ire), fuel limitations, associated access limitations, and persistence. Space-based intelligence collection was soon viewed as a possible solution, and the CIA's first space-based program, *Corona*, became a reality.[49] By design, space-based intelligence demanded close integration of collection and dissemination technologies, seen in the form of electro-optical (EO) imagers (sensors); unhindered and unchallenged access to Soviet territory (via orbit); and ground-to-satellite and satellite-to-ground communication links for command and control of the sensors and platforms. Most importantly, in conjunction with the U-2 flights, the information gleaned from *Corona* confirmed the missile-gap's fallacy and influenced subsequent defense budget allocations.[50] The advent of space-based intelligence marked the dawn of permanent strategic intelligence collection during peacetime, elevating military strategy as a full-time endeavor and thus creating a perpetual need for information gathering. Persistent, global, rapid, and exquisite information suddenly empowered policy makers to make national security decisions at all stages of conflict, which in turn levied additional information requirements and raised expectations for decision-making, strategy, and war in the future.

Space capabilities were soon augmented by the integration of smaller, faster, and relatively cheaper computers capable of processing larger amounts of data in shorter periods of time. In effect, processing capacities increased exponentially and computing technologies, once proprietary, became integral in daily lives. Thus, both military and civil information capabilities surged, predominately through space and cyberspace. *Militarily, space and cyberspace came to represent the two primary information domains enabling global force projection, force employment, and C2.*

[49] T.A. Heppenheimer, *Countdown: A History of Space Flight*, (New York, NY: John Wiley and Sons, 1997), 141.
[50] Brugioni, 244-245.

Force Projection and Employment

In paving the way for gaining an advantage, strategy sets information requirements and decision points. However, another secondary role of strategy—yet unmentioned—is its influence on force development, projection, and employment. Evaluating the expanding requirements for force structures and application throughout the past two centuries and their relation to available information technology provides an interesting connection between strategy and information in war.

Historical methods of power projection and force application relied less on information collection and dissemination technologies than today, in large part due to technical limitations indicative of the time. Up to and including the early 1800s, power projection capabilities on land remained linked to infantry mobility, influencing timelines, distances, force sizes, and sizes of fronts. Maritime force projection differed in its reach, of course, but vessels operated autonomously, fostering a culture of independence where ship captains harbored complete authority over their crafts. Most notably, nascent communication technologies, described previously, ultimately restricted force projection and employment options over land and sea. Indeed, Martin Van Creveld's depiction of communication technology as the "stepchild of war" through the early 1800s accurately portrays the realities strategists encountered.[51]

The operationalization of the railroad and telegraph changed the face of strategy. Lines of communication, supply, and logistics enlarged considerably, and force sizes grew accordingly. By the mid-1800s, commanders were challenged with fronts spanning hundreds of miles. Additionally, force sizes on battlefields had increased from 30,000 men in the year 1650 to 150,000 in 1806 to an unprecedented 460,000 by 1866 in the battle at Königgrätz.[52] The sheer scale of war provoked Moltke the Elder to appreciate the need for maintaining and orchestrating operational reserve units to address contingencies from a continental perspective. Certainly, the notion of an operational level of war could not exist without integrated communication and transportation networks. Mobilized warfare assumed a new importance, and its process was made possible by the unification of rail and telegraph.

---

[51] Martin Van Creveld, *Command in War*, (Cambridge, MA: Harvard University Press, 1985), 104.
[52] Van Creveld, 104-105.

Air power's introduction to war in the early 1900s once again altered strategic thinking in terms of force projection and application. Strategy suddenly incorporated a third and relatively unrestrained dimension into its span of control. Previous increases in force size, firepower, and scale now were now augmented by the speed and unobstructed reach inherent in the air domain. The interwar period between WWI and WWII saw advancements in industry and technology combine to produce a staggering growth in air power development. Concurrently, telephonic networks, radio, and radar technologies all achieved full-scale implementation prior to and during WWII. Newly available information technologies empowered air power's potential by enabling long-range communication and coordination across land, sea, and air—a near impossible task at the turn of the century. As a result, comprehensive force projection and employment considerations transitioned from a continental scale to a global outlook, once again reshaping the scale of war and influencing future force development requirements, projection expectations, and employment assumptions.

The necessity of global reach embodies a common viewpoint in today's security environment. In essence, the US defense strategy (to include force structure) is generally built on a concept of global mobility and engagement. As a result, since WWII, the US defense posture has remained largely forward deployed, organized through the establishment of geographic combatant commands. As it stands, force projection and employment capabilities are underscored by vast global communication networks made possible through the exploitation of all operational domains: land, sea, air, space, and cyber. Indeed, current strategies are contingent upon the continuous availability of these communication networks.

The ability to orchestrate such a large displacement of force relies on effective command and control structures, recalling a third foundation of victory: decision-making. Information technology, force projection and employment requirements (as dictated by strategy), and command and control fulfill the foundations of success in war. Needless to say, the concurrent expansion information technology and the scale of war (strategy) is not a coincidence, and neither is their relationship to evolving command and control mechanisms.

Command and Control

The utility of C2 originates from the beginning of human conflict.[53] Command and control functions encompass prioritization, coordination, training, discipline, administrative oversight, and overall direction of forces toward a determined goal. However, while its functions are eternal, the role of C2 in strategy development and implementation "increases with the sophistication of forces." Thus, in accordance with the expansion of force projection and employment described above, C2 "dimensions have grown exponentially in modern times, especially since 1939."[54]

Progression of C2 functions and associated information requirements coincided with advancements in information collection and dissemination technologies, which in turn coincided with the profound increase in force structures. Concurrent with force structures through the mid-1800s, C2 was performed primarily (and sometimes exclusively) by a central authority.[55] The glacial pace of communication technology developments up to that point in time cultivated the primacy of military genius in command. The quality and quantity of information varied, and oftentimes proved contradictory.[56] Thus, heavy reliance was placed on the commander's ability to filter information and extract actionable intelligence, as codified by Clausewitz. Instead of building C2 systems around information processing, then, early commanders compensated for information deficiencies by first standardizing force structures and movements on the battlefield and later forming staff elements to curtail uncertainty in guiding a wider range of forces.[57]

The Romans constructed one of the most effective solutions to problems with command (lack of information and potentially incompetent commanders) and their approach was replicated in various forms for over a thousand years. The Romans, and those who mimicked them, relied less on technical superiority and instead emphasized "standardized formations, proper organization at the lowest level, a fixed repertoire of tactical movements, and the diffusion of authority throughout the army in order to greatly

---

[53] Van Creveld, 9.
[54] Van Creveld, 1, 6.
[55] For example, Napoleon and Marlborough shared an innate ability to visualize the battlefield and direct forces in accordance with their own interpretation of the environment. See Michael Howard, *War in European History*, (Oxford: Oxford University Press, 1976), 83.
[56] Van Creveld, 67.
[57] Van Creveld, 97.

reduce the need for detailed control."[58] This scripted approach proved sufficient for smaller armies that operated in relatively close proximity to one another, allowing a commander to fight alongside his army. Intelligence collection was ultimately the commander's responsibility, and even if that proved insufficient, the army could function—and even achieve victory—with regularity.

This approach did not imply that information was irrelevant, however. In fact, the opposite was true. By building a modular force structure that permitted the interchange of units with minimal dissonance, armed forces were able to facilitate information flow by reducing the "frequency with which information had to be passed between the army and its headquarters," thereby "extending the range over which information could usefully be sent."[59] By the 1800s, commanders no longer fought on the battlefield and instead retracted to managing the war from afar as though they were embroiled in a game of chess. In his sweeping campaigns of Europe in the early 1800s, Napoleon increasingly relied on messengers to collect specific information on his own forces and those of the enemy to assist his strategic decisions. These informed decisions could in turn be transmitted to various units at Napoleon's discretion and carried out with minimal explanation.

The breakdown in the modular system of scripted warfare occurred toward the final stages of Napoleon's march across Europe. As indicated, force sizes were growing rapidly, and existing C2 structures could no longer control the actions of the forces they led.[60] Napoleon's army at Austerlitz in 1805 boasted 85,000 men, whom he commanded effectively, but the following year, he failed to maintain control of his 150,000-man force at Jena. By 1813, Napoleon's span of influence only reached one of his three armies engaged at Leipzig, a combined force totaling 180,000 soldiers.[61] Not surprisingly, communication technologies had not yet entered the scene to support the new scale of war. When the railroad and telegraph did emerge as viable options for command and control several years later, Napoleonic warfare was shelved as a relic of history.

[58] Van Creveld, 56.
[59] Van Creveld, 61.
[60] For a brief review of European force size increases in the 1800s, reference Howard, 99-100.
[61] Van Creveld, 104-105.

As discussed, the mid-1800s witnessed the birth of the operational level of war. The gradual evolution of C2 systems moved from unit-driven cohesion to army cohesion made possible through command staffs. War was no longer resolved in a single battle or a succession of battles—it was now realized through a series of seemingly disparate engagements across a large geographical expanse. Consequently, in his campaign of 1870, Moltke realized the need to unite his forces "in space and time to achieve the overall aim."[62] The operational level of war, then, demanded a C2 structure that enabled large forces "to march separately but fight jointly," placing greater prominence on accurate intelligence and integrated communications between dispersed units.[63] When rail and telegraph capabilities dominated the landscape, C2 requirements moved beyond the immediate battlefield to the coordination and synchronization of logistics and force projection. The Prussians, led by Moltke, resolved this issue through the formation of command staffs.

Changes in force application also drove greater coordination requirements on the battlefield. In particular, the advent of breech-loading rifles created a new impetus for unit coordination. The new rifles enabled a more effective defense against traditional troop formations that sought to suppress linear enemy advancement through coordinated and predictable salvos. Breech-loading rifles allowed soldiers to fire from behind cover and thus led to a wider and less structured dispersion of troops in battle. This restructuring of ground combat negated a significant level of control exerted by junior officers by effectively removing soldiers from view of each other and of their commanders.[64] Sun Tzu's timeless adage of knowing oneself and the enemy thus experienced a new twist, ultimately influencing strategic decision-making by the commander and general staff based on disposition of forces. The lack of tactical communication technologies plagued subsequent armies until the radio emerged in WWII.

The convergence of information collection and dissemination technologies with force projection and employment requirements in the twentieth century led to insatiable

[62] G. Isserson, "The Evolution of Operational Art," *The Evolution of Soviet Operational Art, 1927-1991: The Documentary Basis*, Vol. 1. *Operational Art, 1927-1964,* trans. Harold S. Orentstein, (London: Frank Cass, 1995), 60.
[63] Van Creveld, 105.
[64] Howard, 102.

demands on C2 functionality. The number of available forces, the firepower and range of their weaponry, incredible speeds of maneuver, and scale of conflict all placed immense pressure on C2 structures to devise and orchestrate strategies capable of optimizing outputs. Airplanes, radios, radar technology, satellite systems, and computers fed a growing demand for information to overcome unparalleled complexities in warfare.

Today, strategy, decision-making, and information capabilities and requirements have reached such a symbiotic state that they form a single entity. Most notably, information technologies have advanced and multiplied to the point where weapon and C2 system functionality are predicated on the availability of information networks, creating an entirely new dimension in strategy. In the Information Age, information collection, processing, and dissemination have reached near-instantaneous speeds, and decision-making now fluctuates between man and machine. Thus, *whereas historical C2 systems and force structures existed to compensate for informational deficiencies, modern C2 systems and force structures cannot exist without information networks.* (This transformation is explored more closely in Chapter 2.)

Broad Implications for National Security and Defense

These three factors (information technology, force projection and application requirements, and C2) all shaped the value of information and its characteristic qualities in war. As humans progress further into the twenty-first century, these factors will continue their transformative behavior but will always retain their relational structure. In this regard, two final considerations deserve mentioning before undertaking a deeper examination of Information Age warfare. The first highlights the social changes resulting from a mass proliferation of information technologies, their relationship to national security, and their invariable influence on the conduct of war. The second notion briefly returns to the enduring qualities of human nature and its manifestation in the present age.

Political and Public Expectations

In assessing war's nature, Clausewitz determined three intertwined elements that influence its adaptive appearance: passion, chance, and reason.[65] The latter two elements

[65] Clausewitz, 89.

involve the commander's skill and political objectives, respectively, while the first relates to the people's will or desire for war. Information's association with the commander and military genius affects decision-making, but it also plays an increasing role in generating public support and setting national objectives for war.

After WWII, information technologies slowly transitioned from the propriety of governments to the private sector, laying the expectations for Information Age warfare. Mass proliferation of information technologies spread across the globe, binding dispersed populations and distorting borders. Moreover, the resultant globalization of communications and commerce redefined national security considerations, and two influential factors surfaced. The first factor unveiled itself after Desert Storm in 1991 and persisted as a direct result of mass communications. In Desert Storm, the public witnessed an incredible display of firepower with astonishingly minimal loss of life. In this sense, networked information systems enabled the employment of precision-guided munitions (PGM) from standoff locations, reigning intense yet controlled firepower in select doses and effectively limiting collateral damage. Similar communication networks disseminated the new weapon effects throughout the globe, raising public and political expectations on the future conduct of war. At the same time, the Soviet Union collapsed, ushering in a new geopolitical era and the end of the Cold War. As the world's only remaining superpower, the United States refocused its emphasis on force application in stabilizing world affairs. Thus, a new strategy of coercive diplomacy evolved in the post-Cold War era, fueled by increasing demands for shorter conflicts and reduced acceptance of civilian deaths. In the Information Age, strategy now incorporates a broader influence of public sentiment when conducting war. Whereas the impetus or desire for war has always gained its momentum from national will (in democratic societies), the *conduct* of war is increasingly dictated by the public, and, by representation, its politicians.

Public perception places greater responsibility on centralized command and control to confine force application within the acceptable parameters prescribed by the population and their representatives. Due to the advent of weaponry with such overwhelming firepower and precision, how war *looks* is now just as important as what war accomplishes. This demand also increases the need for greater transparency, made possible through information systems and their ability to collect and disseminate

information. Strategically, then, information drives decision-making, command and control, force projection and application capabilities, as well as public narratives for support, justification, and applicability.

The second national security factor addresses a fundamental impetus for war: the pursuit or protection of national interests. Globalized networks, made possible through space and cyber capabilities, form the fabric of national security and prosperity. In telling fashion, the 2015 National Security Strategy considers a "catastrophic attack on the U.S. homeland or critical infrastructure" as a "top strategic risk" to its interests.[66] Similarly, the 2010 Joint Operating Environment (JOE) provides the following synopsis of space and cyber capabilities and their relationship to US security:

> Our society's very way of life has come to depend fundamentally on the use of cyberspace. In much the same way that we depend on our highways and the oceans, we rely on networks pieced together through the electromagnetic spectrum to conduct business, purchase goods, entertain ourselves, and run our basic utilities…. [Likewise], the U.S. relies heavily on space-based assets to observe the operating environment and orient far-flung forces at global distance in highly distributed networks. This dependence creates both advantage and vulnerability.[67]

Therefore, the expansion of information technologies beyond military utility has altered the character of war in terms of force projection and application, command and control, and national security. Strategy, then, must remain focused on gaining leverage in a world dominated by mass communication and enhanced public perception of force application, all while securing those capabilities that simultaneously support prosperity and enable national defense.

Feeding the Machine—The Balance between Strategy and Information

The proliferation of information collection and dissemination technologies plays to human sensibilities by providing opportunities to understand as much as possible and reduce an intrinsic fear of the unknown. This inevitable reaction to such technology has led to a state of information saturation and a potential readjustment in the concepts of centralized control and decentralized execution. Information technology and networked

[66] White House, *National Security Strategy*, (Washington, DC: White House, 2015), 2.
[67] United States Joint Forces Command, *The Joint Operating Environment 2010* (Suffolk, VA: Joint Futures Group, 2010), 34, 37.

communications create a temptation for decision-makers to place informational demands that undermine the effectiveness of their strategy. *The capability to do so does not create an imperative*—more information is not always better or required.

The enduring relationship between strategy, decision-making, and information coupled with the convoluted networking of communication technologies characteristic of a globalized society generate two challenges for modern strategists. First, while the intent is not to focus directly on the cognitive processes and nuances of decision-making, it ultimately emphasizes human leadership in determining and prioritizing information needs according to the decisions incorporated within strategy. As indicated, sound strategy exists to filter the type and quantity of information decision-makers need. Consequently, strategists in the twenty-first century must reconsider the realities of war, the primacy of strategy, and the efficacy of decision-making. However, a concern rests in an overreliance on information and technology that supersedes or even supplants sound strategy development and decision-making prowess, thereby disrupting the balance between strategy, decision-making, and information.

Relatedly, after WWI, the United States defense establishment has shown a tendency to believe that technology ultimately transcends any geopolitical issue. Since the overwhelming success of Desert Storm and the dissolution of the Soviet Union, US technological superiority has remained unmatched while engaging progressively weaker adversaries. As a result, technological advancements flourished with little resistance, enabling widespread acceptance of sophisticated force employment and augmentation capabilities with only a peripheral demand for contingency planning in the event of their loss. In a relatively permissive operating environment, such a technological dependency allows for a lesser regard for the intricacies that enable it. Thus, in a time of great technological change, strategists must strive to understand the potential capabilities, limitations, and susceptibilities inherent in their desired way of war, particularly as they plan against near-peer adversaries who may have the ability to neutralize its advantages. Indeed, perhaps more than ever before, the onus is on strategists to understand geopolitical implications in building a manageable, appropriate, and effective strategy-decision-making-information continuum.

Conclusion

War is and will remain an output of human nature. Fears of the unknown and a central desire to control outcomes infiltrate human interactions. Political discourse only heightens these tendencies, as states vie for strategic advantages to secure their interests and ensure future prosperity. When war ensues—and it inevitably will—the collision of self-preserving entities yields chaos. Strategy, as a process and product, exists to provide a deliberate roadmap for prioritizing objectives and gaining the advantage over an opponent. To this end, sound strategy identifies opportunities for decision-making, which in turn drives information requirements. The strategy-decision-making-information structure lays the groundwork for all activities in war, and only varies in its scale as war's character changes.

Historically, information was required to develop strategy and make related decisions, and that trend remains steadfast. Nevertheless, the character of war was such that decisions were made independent of the actual fighting force. Information was scarce—a prized commodity—and a lack of information did not necessarily prevent an army from engaging in battle (although collection of information could generate an asymmetric advantage). Over time, armies outgrew their commanders' abilities to control them, and the scale of war encompassed larger geographic areas, requiring greater considerations in the placement of forces in time and space, relative to one another. The resulting complexities in strategic and operational level planning demanded an increase in available communication capabilities, and the twentieth century finally saw the convergence of force projection and application requirements with an overabundance of information collection (characterized by access and method) and dissemination (defined through speed and reach) capabilities. After WWII, the advent of space operations and computer technologies marked a pivot point between historical and Information Age warfare: that of networked forces designed to operate with perpetual information, outside of human decision-making and tied directly to the functionality of the weapon systems themselves. The ability to circumvent limitations of available communication technology by disaggregating forces to achieve maximum effect became an elusive concept in modern warfare. In the twenty-first century, even the smallest armed contingent relies on a broad and intricate network of information systems to enable its functionality, creating

susceptibilities foreign in their existence and scale to armies and commanders of the past. Indeed, in the Information Age, the impetus for information control and information superiority assumes new meaning. With a broad baseline of war, strategy, decision-making, and information set, key characteristics of the Information Age—relative to the Industrial Age—and their relevance to twenty-first century warfare now fall under investigation.

Chapter 2

The Information Age and Emergence of Infospheres

Rapidity of modern means of communication, the sureness of various means of transportation, and the accessibility of all parts of the world to aircraft, which have been developed in an incredibly short space of time, make it absolutely necessary that we organize to meet modern conditions. Our various means of national defense must be accurately coordinated because the next contest will increase the swiftness with which decisions are reached and the nation that hangs its destiny on a false preparation will find itself hopelessly outclassed from the beginning.

- William "Billy" Mitchell

Every new medium transforms the nature of human thought. In the long run, history is the story of information becoming aware of itself.

- James Gleick

If the US intends to preserve its ability to conduct its desired way of war, it is important to first understand the characteristics and origins of its preferred methodology and then determine whether it is postured to sustain it. To this end, and building from the theoretical construct of war established in the first chapter, an analysis of the US military's progression from the Industrial Age to the Information Age follows. The intent is to evaluate the evolution of war's character across the two eras to formulate a theoretical portrayal of modern warfare from the US perspective. The analysis then proceeds with a theoretical description of the information environment, or *infosphere*, exploring its effect on military operations and information control in the twenty-first century. A preliminary assessment indicates the US military is not fully optimized for Information Age warfare and therefore requires conceptual (first) and physical transformation.

Of course, the possibility of change breeds uncertainty in any bureaucratic organization. Organizations seek to minimize uncertainty to maintain their purpose and structure, which create stability and ensure the delivery of outputs for which they were designed.[1] Moreover, to an entity pursuing some measure of control over its fortune, uncertainty can induce anxiety. Nevertheless, change—or at least the *perception* of change—remains one of the few constants in the human experience.

---

[1] Stephen Rosen, *Winning the Next War: Innovation in the Modern Military*, (Ithaca, NY: Cornell University Press, 1991), 2.; Barry Posen, *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars*, (Ithaca, NY: Cornell University Press, 1984), 224.

The progression of the Information Age has generated a level of uncertainty in the US defense establishment, and rightfully so. Built from an Industrial Age mindset, military organizations, operations, and acquisitions function within hierarchical structures that value consistency and predictability in achieving predetermined results. The Information Age, in contrast, tends to value fluidity, persistent and dynamic change, and unpredictability, stemming from the rapid development and proliferation of information technologies. A divergence between organizational function and strategic landscape emerges, pitting an Industrial Age force against an Information Age world. Because strategies exist to gain an advantage and exert control over an opponent or environment, such a dichotomy can theoretically prove catastrophic. Thus, the uncertainty of the Information Age to an Industrial Age force invariably leads to anxiety over the prospective inability to gain the advantage in future conflicts.

As an Industrial Age defense apparatus attempts to understand the characteristics of Information Age warfare, several questions come to the fore. What are the similarities and differences between Industrial Age and Information Age warfare? What enduring concepts connect the two epochs? Is the Information Age simply an output of an industrial society? What specific artifacts and concepts define the Information Age? How do Information Age characteristics affect strategy? Gregory Bateson summarized Claude Shannon's groundbreaking information theory from 1948 as "Any difference that makes a difference."[2] Indeed, by assessing these questions, national and military strategists can better recognize *differences that matter* and adapt accordingly. Over time, relevant differences between industrial- and information-centric methodologies will materialize, but recognition of stability amidst change allows for manageable re-posturing now in anticipation of future transformation.

Analysis reveals that while differences abound, continuity between the ages not only exists but also provides a familiar path for transformation. Conceptually, each age embodies a different perspective of the same world—two paradigms, one an offshoot of

[2] George Dyson, *Turing's Cathedral: The Origins of the Digital Universe*, (New York, NY: Vintage Books, 2012), 3. Claude Shannon developed his information theory from the designation of a "fundamental unit of communicable information, representing a single distinction between two alternatives." In digital communications, a binary language creates an opportunity for such options, where "the only difference that makes a difference is the difference between a zero and a one." In reviewing Industrial Age and Information Age characteristics, the only differences that make a difference are those that render traditional strategies, organizational processes, or capabilities ineffective in gaining leverage and control.

the other. Physical realities remain intact, and the principles of war continue unabated. Pragmatically, though, an unavoidable reliance on an *information environment* (or *infosphere*, described later) for force projection and force employment constitutes the most characteristic feature of the Information Age. Additionally, networked communication infrastructures have created a situation where quantitative and indiscriminate strength indicative of Industrial Age warfare is gradually being replaced by qualitative power, manifested through an inverse relationship between reduced force sizes and increased potency (see Figure 2). Most recently, this trend was propelled by a growing capability and subsequent desire to reduce risk to friendly forces and maximize effects against the enemy, all while minimizing collateral damage. Of note, Figure 2 illustrates a trend in Western society's approach to warfare and is not necessarily a universal depiction.

To secure this approach to war, strategists must take great care in assuring access to information networks that enable precision operations demonstrative of the new era—a cornerstone of information control. A failure to do so will create situations where the new way of war can no longer persist, preventing precision warfare and requiring an increase in mass and indiscriminate violence—a task unsuited for smaller, more exquisite forces. Fortunately, because certain physical systems and domains bridge each period (i.e., space), continuity forms through reassessing existing technologies and capabilities under Information Age requirements. Ultimately, analyzing key characteristics of the Information Age and understanding how infospheres enable the United States to conduct its preferred method of war provide context for establishing a more appropriate definition of information control—the central element of Information Age warfare.

A Comparison of Kindred Ages

As stated, the industrial and information ages represent periods in history with different perspectives on how the world works, and, ultimately, how humans can exert control within that world. In particular, the two paradigms vary in how strategic success is defined and the assumed availability of information in achieving (or establishing) objectives. Notably, the Information Age is a direct output of a mature industrial base. In fact, the new age coalesced from an insatiable quest for more information, a constant

struggle for decision makers during the Industrial Age. Ironically, although not surprisingly, an overabundance of information—characteristic of the Information Age—has not quenched the demand for it. If anything, the demand signal is greater than ever before, prompted by a deeply imbedded reliance on data and information for routine functionality.

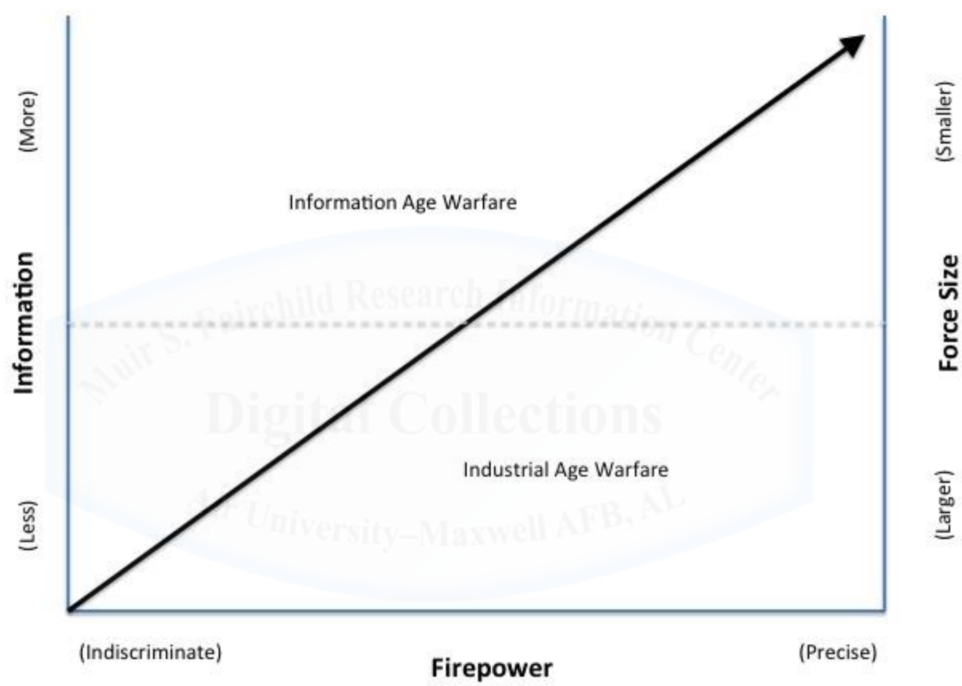

Figure 2: Information, Firepower, and Force Size Relationship
Source: Author's Original Work

To understand the relationship between the two ages, an overview of prevailing characteristics and their influential factors is provided, followed by a brief analysis aimed at extracting key associations that may shape concepts of war in the future.

The Industrial Age

At a societal level, the nineteenth and early twentieth centuries witnessed the full magnitude of mankind's productive and destructive potential. Industrial juggernauts

were able to project their interests abroad, fueled by the demand for greater resources, global (or regional) influence, and a newfound perspective on national security. Steam engines, the conveyor belt, locomotives, the cotton gin, breech-loading rifles, airplanes, thermonuclear weapons, and satellites all developed under the Industrial Age and shaped the way strategists perceived the world. National, military, and civilian organizations formed under this construct, characterized by the preeminence of tangible artifacts, totality, and mass: mass production, consumption, mobilization, concentration, and destruction.[3]

Due in large part to informational deficiencies, the Industrial Age mentality valued structure, redundancy, stability, efficiency, repeatability, and linearity.[4] As previously noted, military formations organized themselves in ways that ensured standardization (in structure and function), a measure taken to compensate for the lack of available communications technologies for inter-unit coordination during battle. War's expanding scope, resulting from transportation and communication technologies such as the railroad and telegraph, challenged C2 methods and gave impetus for the Prussians to implement the general staff. Like military formations, the general staff existed to induce a level of standardization by codifying commander's guidance, disseminating tasks, interpreting intelligence, and coordinating the efforts of a widely dispersed force. In both cases, the need for such standardization and deterministic approaches persisted from increased scales of measurement in production coupled with meager developments in communication capabilities.

Furthermore, industrial societies emphasized manufacturing and expansion, and weapons technologies favored enhanced destructive power. An increasingly technical approach to warfare ensued, a reality that persisted from the Middle Ages, made possible through a combination of engineering, manufacturing capability, and operational necessity. Bigger, faster, and more powerful weapon systems provided armies the means for destroying equally massive formations on the battlefield, and the absence of advanced communication systems for coordination placed a higher priority on brute force to attain

[3] Keith L. Shimko, *The Iraq Wars and America's Military Revolution*, (New York, NY: Cambridge University Press, 2010), 10.
[4] John E. Rothrock, Edward F. Smith, Jr., and John F. Kreis, *The Industrial Age Versus the Information Age: Rethinking National Security in the 21st Century*, IDA Document D-2536 (Alexandria, VA: Institute for Defense Analyses, 2001), 5.

victory.[5] Technical prowess unleashed physical strength inherent in the war machines, and bureaucracy proved the best mechanism for synchronizing ways and means in achieving victory. Thus, tangible metrics of strength, quantity, proficiency, and order formed the industrialist's mindset and decision calculus.[6]

Meanwhile, accurate and timely information remained elusive, or at least inconsistent, and was therefore at a premium. Additionally, any information gleaned contributed to the physical destruction of the enemy. Despite employing organizational designs to alleviate informational deficiencies, commanders consistently sought information asymmetry, as any advantage in information collection could generate decisive results on the battlefield. The dawn of air power in WWI, discussed earlier, offers a key example of armies exploiting new collection technologies as a means for gaining an information advantage to support kinetic engagements. Congruent with Industrial Age thinking, air power matured in the interwar years as a warfighting (and potentially war-winning) capability, and reconnaissance fulfilled an ancillary, albeit critical, role.

World War II and the dawn of the Cold War marked the height of the Industrial Age approach, but they also reveal insight into the underlying motivations (and capabilities) that gave rise to the Information Age. The industrialization of war manifested itself in the ruthless slugfest of WWI, and leaders worldwide vowed to avoid such methodical and relentless devastation. The interwar years between WWI and WWII thus saw a distinct shift in society's view of technology, then seen as a solution to the atrocities of Industrial Age warfare. To some, air power offered a means for circumventing ground combat, and the airplane specifically symbolized a new way of conducting mass warfare and delivering victory (consistent with the age). A state's capability and will to fight were simultaneously held at risk, and the allure of offensive and decisive warfare was found in strategic bombing. By 1945, air power advocates like Guilio Douhet and William "Billy" Mitchell received vindication (posthumously) of air

[5] Industrial Age warfare tends to identify a notion of *strategic victory* through success in battle—if one achieves battlefield success (at the tactical level), the war is won. This mentality elevates the function of combat (physical confrontation) rather than aligning victory with political intentions, which incorporate multiple resources and objectives in shaping the strategic landscape. See Everett C. Dolman, *Pure Strategy: Power and Principle in the Space and Information Age*, (New York: NY, Frank Cass, 2005), 5.
[6] Rothrock et al., 5.

power's potential as bombers delivered two atomic weapons over Japan, forever changing the landscape of war. Notably, nine years prior, Alan Turing conceptualized a Universal Machine, a stored-program computer that could distinguish between data points that mean something and data points that instruct machines to do something. As the atomic bombs were falling over Hiroshima and Nagasaki, Hungarian mathematician John von Neumann and a select team initiated construction of an electronic digital computer based on the designs conceived by Turing.[7] The stage was set for a cognitive transformation that ultimately took decades to appreciate, in large part due to the strict, rigorous, and process-driven culture required for nuclear deterrence.

The culmination point occurred during the first years of the Cold War. Industrial mobilization exploded in United States after WWII, now one of only two great powers left in the war's aftermath. The Berlin Crisis of 1948-1949 crystalized the seeds of distrust between Western powers and the Soviet Union that formed during the war, marking the beginning of an arduous competition that would ultimately wreck a nation and define international relations indefinitely. In 1953, the world witnessed the first thermonuclear detonation, generating a force one thousand times more powerful than the atomic weapons used over Japan eight years earlier.[8] Revolutions in computer technology allowed for unprecedented simulations of nuclear weapons designs and effects, leading to smaller and exponentially more destructive devices. The prospects of nuclear war between the Soviet Union and United States would only increase, placing greater demands on structure, standardization, and predictability in deterrence operations. Mass retaliation aimed at counter-value targets dominated the strategic bias, and both nations mobilized their collective resources to gain leverage over the other, a decidedly futile attempt in total nuclear war.

The penultimate product of the Industrial Age—space-based capabilities—sprang from this geopolitical standoff. As previously discussed, the launch of *Sputnik* sent shockwaves around the world. The space launch confirmed that delivery systems now existed that could transport the new thermonuclear warheads to any point on the globe in less than an hour. From a strategic standpoint, the Soviet Union could theoretically hold

[7] Dyson, ix.
[8] Dyson, x.

the United States at risk, and no technology existed that could defend against ballistic missiles. The demand for strategic intelligence to determine Soviet nuclear capabilities coincided with a new ability to do so, and aerial reconnaissance was soon augmented by space-based collection. Once again, information was at a premium.

More than just satellites (the distinguishable artifacts of space operations), the space infrastructure encompassed the entire spectrum of industrial productivity and national mobilization.[9] Launch vehicles, rocket engines, dispersed ground stations for satellite tracking and C2, computer technology for on-board and distant-end processing, and manipulation of the electromagnetic spectrum (EMS) for rapid, global communications and connectivity comprised the backbone of the space architecture. Furthermore, nearly one in fifty Americans contributed to the US space program in the 1960s and early 1970s.[10] Ultimately, massive industrialization on the planet inevitably moved the Cold War's battleground to the stars, and both states attempted to reach milestones in space to demonstrate their industrial and, by extension, ideological superiority.

The Cold War persisted through 1991, and the Industrial Age endured with it, well beyond its apex. The threat of nuclear war placed immense pressure on the government's ability to stabilize the strategic environment, control escalation, and orchestrate the projection and application of military forces. Guided by a compatible paradigm, strategists attributed significance to the *quantity of things* (e.g., weapons and machines) and the efficient use of said things via repeatable processes designed and executed by specialized (parochial) and hierarchical organizations designed to offset gaps in information that would otherwise facilitate greater economy of force. Thus, the Industrial Age focus on "doing things right" governed the military's approach to national defense and extended the age's lifespan.[11]

---

[9] Physical access to space is only possible through a highly industrialized society. However, access to space *capabilities* requires fewer demands on a state's industrial might. This distinction highlights a key relationship between Industrial Age and Information Age connections, discussed later.
[10] Roger D. Launius, *NASA: A History of the U.S. Civil Space Program*, (Malabar, FL: Krieger Publishing Company, 1994), 70.
[11] Rothrock et al., 24.

The Information Age

The Information Age describes a paradigm that views the world slightly different than its predecessor. Industrial Age tenets such as quantifiable strength, efficiency, decisiveness, linearity, technical proficiency, predictability, and stability shifted to (but were not replaced by) an emphasis on qualitative power, effectiveness, non-linearity, education, sufficiency, flexibility, outputs, and operating through chaos.[12] The crucial factor delineating the two epochs arises from the commonplace accessibility of information to a broad (rather than exclusive) audience, made possible through the rapid proliferation of increasingly complex information technologies at cheaper cost to the consumer. The availability of similar information to government and citizen alike appeared to recalibrate international structures, seemingly leveling the playing field between state and non-state actors. Notionally, individuals were empowered by information, creating amorphous challenges for national defense due to a larger contingent of actors influencing political outcomes. Moreover, Industrial Age control mechanisms no longer dictated security considerations, as military forces could better regulate and optimize firepower based on greater situational awareness. Consequently, concerns over incompatible Information Age concepts permeate a force largely built on Industrial Age priorities.

A closer look at the strategic landscape that developed around the Information Age provides a more comprehensive explanation of how the paradigm shift occurred, if not exactly when. The Vietnam War, Desert Storm, the end of the Cold War, and propagation of globalized communication networks all provided opportunities to challenge the prevailing paradigm. Soon after the advent of the digital computer, thermonuclear bomb, intercontinental ballistic missile, and space technology, the United States—thoroughly embroiled in its competition with the Soviet Union—committed forces to defend South Vietnam against its northern communist aggressors. The US military interpreted the conflict through Cold War and Industrial Age lenses and, empowered by state-of-the-art technology, performed the only way it knew how (and the only way that provided a measurement for success): seeking victory by applying

[12] Rothrock et al., 5.

overwhelming force to destroy the enemy's capacity to fight.[13] The fact that Vietnam was engaged in an emotional civil war was shrouded by the larger concern over nuclear deterrence. The geopolitical environment was not conducive for a traditional, Industrial Age strategy, and tactical victories failed to generate the strategic advantage strategists assumed they would gain. Strategic failure in Vietnam demoralized the US defense establishment and disenfranchised conventional perceptions of war.

As the United States and North Vietnam fought each other from incongruous angles, computer and information technologies inconspicuously accelerated in the background. Motivated by fears of a surprise nuclear attack, decision makers demanded persistent coverage and analysis of adversary capabilities and intentions, and information systems were designed to meet the growing requirements. As examined, space systems, originally employed for strategic reconnaissance, soon introduced the notion of global information dissemination through mass communication.[14] In 1967, Marshall McLuhan remarked, almost prophetically, "Man the food-gatherer reappears incongruously as information-gatherer…. In this role, electronic man is no less a nomad than his Paleolithic ancestors."[15] McLuhan's commentary invoked the inkling of a new way of framing human interactions, but the world, locked in a Cold War vice, would not awaken to this fundamental premise until after 1991.

The year 1991 marked a fundamental turning point in the mentality of industrialized societies and militaries, if such a point ever existed. Specifically, Operation Desert Storm and the end of the Cold War combined to break the established mold and helped bring substance to a new paradigm gestating under the surface. The US military, determined to rectify its failures in Vietnam, planned and executed Desert Storm with the intent of creating strategic paralysis by destroying key Iraqi command and control capabilities. Precision guided munitions, aided by newly acquired space-based capabilities, allowed the military to concentrate firepower in condensed but devastating fashion and demonstrated to the world (including the public) that previous ways of war were obsolete. Furthermore, information collection and dissemination through

---

[13] Martin Van Creveld, *Command in War*, (Cambridge, MA: Harvard University Press, 1985), 259.
[14] Donald Cox and Michael Stoiko, *Spacepower: What it Means to You*, (Philadelphia, PA: The John C. Winston Company, 1958), 88-89.
[15] James Gleick, *The Information: A History, A Theory, A Flood*, (New York, NY: Vintage Books, 2011), 8.

sophisticated space-based communication architectures created an asymmetric information advantage and led General McPeak to categorize the event as "the first space war" at its conclusion, setting substantial expectations for future conflicts.[16] Months later, the Soviet Union collapsed, marking an abrupt end to the Cold War. The dominant strategic imperative for national defense suddenly vanished, and the geopolitical landscape received a violent jolt. Information technologies, having already infiltrated critical national infrastructures of industrialized nations, provided a means for unifying the globe in the new unipolar environment. By the end of 1991, the existential threat was gone, and warfighting capabilities had reached a new height in terms of intelligence collection and dissemination, firepower, accuracy, precision, and reach—made possible through the implementation of advanced information systems.

The suddenness by which geopolitical and technological changes took place sent reverberations throughout world and allowed for the acceptance of a new paradigm. After Desert Storm, national defense pundits concluded that US military defeat in Iraq was implausible, and Robert Citino described the war as "the most successful campaign in US military history."[17] Declarations of a revolution in military affairs (RMA) surfaced almost immediately after the war, and impulsive conclusions that information technologies would reduce the "proverbial fog of war" formed the mantra of RMA enthusiasts. Richard Hallion claimed, "The combination of the lethality of modern air weapons, coupled with the *freedom of maneuver*, range, precision, and sustainability of air attack, has revolutionized war" (emphasis added), and Jacob Kipp ultimately summarized the RMA as "the shift from mass industrial warfare to information warfare."[18] The US military, just as surprised at its swift victory as the rest of the world, was confidently given "a green light to continue along the same path" in preparing for future conflicts.[19] What the RMA and defense establishment failed to consider, at least holistically, were the unique geopolitical conditions that gave rise to the war and the

[16] General Merrill McPeak, Air Force Chief of Staff, address to the National War College on DESERT SHIELD/DESERT STORM, 6 March 1991. Quoted in "The Synergy of Air and Space," *Airpower Journal*, Summer 1998, 7.
[17] Shimko, 76-77.
[18] Shimko, 9, 12, 14.
[19] Shimko, 2.

implications of the undoubtedly temporary unipolar environment that ensued.[20] The Information Age came to fruition in this context.

In many ways, however, a noticeable global information revolution did occur. For the first time in history, human demands for information finally had a complementary supply line, and soon information dissemination capabilities surpassed man's ability to ingest it. Consistent with human desires, the demand signal for more information strengthened, and the insatiable supply-demand relationship grew exponentially. In 2002, Eliot Cohen noted:

> One might suggest that a second communications revolution is now upon us [the first taking place during the American Civil War and the advent of the telegraph], in which a further quantum increase in the amount of information that can be distributed globally has occurred, and the role played by that information in all of civilized life will again transform society and ultimately the conduct of war.[21]

A clear example of technology's increased accessibility and global interconnectivity lies in the tremendous growth of Internet access over the past 20 years. In 1995, nearly 16 million individuals enjoyed Internet connectivity. Five years later, accesses jumped to 300 million. Today, the Internet plays host to nearly 2.5 billion users, each of whom gains access through multiple media devices (e.g., smart phones, televisions, computers, and tablets).[22] From a warfare standpoint, the impacts of this communication boom are most clearly illustrated by comparing satellite communication (SATCOM) bandwidth capabilities between Desert Storm and Operation Iraqi Freedom (OIF) twelve years later. In 1991, SATCOM bandwidth requirements in Desert Storm approached nearly 100 mega-bits per second (Mbps).[23] In 2003, during OIF, that number skyrocketed to 2,400 Mbps, an increase of 240%. By 2010, only seven years later, mission requirements

---

[20] Hallion's conclusion, highlighting the military's freedom of maneuver in Iraq, essentially projected a reality based on specific circumstances in Desert Storm on all future conflicts in the new age. This generalization represents a potentially detrimental assumption in the Information Age as the United States postures itself against more formidable opponents.

[21] Eliot A. Cohen, *Supreme Command: Soldiers, Statesmen, and Leadership in Wartime*, (New York, NY: Anchor Books, 2002), 6.

[22] Internet World Stats, "Internet Growth Statistics: And the 'Global Village' Became a Reality," http://www.internetworldstats.com/emarketing.htm (accessed 25 February 2015).

[23] By comparison, the data rate of the telegraph in the mid-1860s was approximately 8 to 10 words a minute. See Van Creveld, 108.

exceeded 14,000 Mbps, representing a 583% increase from initial OIF demands and a staggering 1,400% upsurge from Desert Storm.[24]

The twenty years that followed Desert Storm shaped the contours of the Information Age. In that time, several key factors contributed to the mentality that permeates the world today. First, control of the development and distribution of information technologies moved outside government control to the civilian sector, and advanced capabilities increasingly spread beyond the realm of national governments. Space-based capabilities such as positioning, navigation, and timing (PNT); terrestrial and space weather forecasting; infrared (IR) detection; global SATCOM (data relay, Internet routing, cell phone communications, TV, etc.); and remote sensing for agricultural and oceanographic analyses were incorporated into national infrastructures. In particular, PNT—a function of the Global Positioning System (GPS)—expanded from an exclusive military enabler to a cornerstone of international commerce, transportation, and electrical power.

Second, since 1991, US technological superiority remained unmatched while its chosen adversaries became progressively weaker in each subsequent conflict. The end of the Cold War left the United States as the world's sole superpower, and the strategic landscape soon led to debates in the US government on the proper role of force—influenced by the newly realized capacity for unleashing potent yet condensed firepower anywhere on the globe—fueling its propensity for electing to engage in less traditional conflicts.[25] In such a situation, unchecked success inadvertently increased expectations for further success. New ways of war emerged in this global laboratory, headlined by catch phrases such as "net-centric warfare" and "information dominance." The impetus behind the new approaches, however, proved nebulous, and force structures remained aligned with traditional concepts of war. Indeed, "net-centric warfare . . . was not tied to a specific opponent in the same way that AirLand Battle in the 1980s focused on the Soviet Union." As Keith Shimko adeptly surmised, "In the absence of a credible threat, military planners lack the information, resources, and motivation that usually drive

[24] Benjamin D. Forest, "An Analysis of Military Use of Commercial Satellite Communications" (master's thesis, Naval Post Graduate School, Monterey, CA, 2008), 1, 12.
[25] Dag Henriksen, *NATO's Gamble: Combining Diplomacy and Airpower in the Kosovo Crisis 1998-1999,* (Annapolis, MD: Naval Institute Press, 2007), 64.

successful innovation . . . and the sense of strategic urgency diminishes."[26] Therefore, the US military gradually built a reliance on information networks in support of its desired approach to warfare, and in so doing, created a susceptible target for adversary exploitation. While America lacked a distinct adversary against which to focus its defense efforts, the rest of the world (including state and non-state actors) had America in its sight.

Third and finally, the geopolitical and technological environment allowed state *and non-state* actors to focus their attention on defeating the single great power through asymmetric attacks, creating a new security dilemma in the minds of US leaders. Globalization of information systems gave rise to the global terrorist, as ideologies spread through virtual networks to anyone who could access them. Terrorists, their recruits, and future prospects were mobilized by shared ideas, many of which denounced US hegemony in the wake of Desert Storm, and states lacked the traditional capacity to combat the new, non-state threats—governments no longer controlled access to the technologies that elevated the non-state actors to threat status.

From a state perspective, China's rise presents an entirely new factor in modern warfare, as the international system gradually rebalances itself through bipolar competition. Perhaps no other country placed higher significance on Desert Storm than China, who closely observed US actions during the war and began referring to the conflict as "the great transformation."[27] Desert Storm had such profound implications that the Chinese completely overhauled their defense strategy from defeating the United States with overwhelming numbers to seeking asymmetric advantages through information warfare. In 1999, two Chinese colonels articulated a new doctrine based on the realization that "the enemy country can receive a paralyzing blow through the Internet" and planned to counter their enemies by taking "advantage of weaknesses created by an adversary's seemingly superior conventional capabilities" via "information dominance."[28] Senior US military officials concluded that China would seek to dominate

[26] Shimko, 129-130.
[27] Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, (New York, NY: Harper Collins, 2010), 49.
[28] Clarke and Knake, 49-51.

the strategic environment by neutralizing US space capabilities and controlling its cyber networks.

The Information Age thus progressed under a series of geopolitical and technological influences. In relation to the Industrial Age, the Information Age formed as a worldwide phenomenon under similar concepts of mass with added dimensions of rapidity, described from information perspectives such as mass and rapid communication, distribution, access, consumption, and collaboration. Conceptually, the world transformed from a production resource to an information reservoir. “We see now that information is what our world runs on: the blood and the fuel, the vital principle,” James Gleick asserts. “The whole universe is thus seen as a computer—a cosmic information processing machine.”[29] Soon, a new way of war emerged—replete with its own assumptions—characterized by the projection and employment of rapid, global, and precise lethality. Military forces could suddenly create overwhelmingly devastating effects through refined and limited quantities across a wide range of attack vectors. At the same time, global and civilian-driven proliferation of information technologies, a unipolar environment, and the rise of state and non-state powers combined to create a dynamic and increasingly unpredictable world. Consequently, analysts of the Information Age—an era still in its infancy—are quick to conclude that concepts of non-linearity, effectiveness, qualitative (relative) power, sufficiency, education, versatility, and chaos oftentimes carry more weight than their Industrial Age counterparts of linearity, efficiency, quantitative strength, necessity, training, structure, and stability. In the end, whereas the Industrial Age mindset emphasized “doing things right,” the Information Age mentality, influenced by experiences in Vietnam and more recently in Afghanistan and Iraq, shifted its focus to “doing the right thing.”[30] In sum, the paradigm shift was empowered by the establishment of global, near instantaneous, and accessible information collection and dissemination capabilities.

[29] Gleick, 8, 10.
[30] Rothrock et al., 24.

Continuity and Change Between the Ages

Because both ages describe two different paradigms, it is difficult to pinpoint a specific time when either began or concluded. In essence, the presumed fall and rise of each epoch is better described as a gradual transition, influenced by innumerable factors and complicated by the fact that the second age never completely subsumed the other—it is a direct descendent of it. Furthermore, the geopolitical and technological environments that helped initiate the Information Age developed in a way that prevented sound analyses of what actually transpired and how it influences—or even enables—the way the United States expects to fight in the future.

By holistically viewing key factors that shaped both paradigms, relevant areas of continuity and change emerge that may help strategists better prepare for future conflict. First, the Information Age is not as disruptive to traditional ways of war as experts first imagined. In fact, many features of the period find comparisons throughout history and therefore effect change in war's character rather than its nature. Furthermore, a strong industrial base and its traditional mindset maintain a prominent place in the twenty-first century—*the Information Age could not exist without them*. Second, the Information Age does offer a distinguishing artifact that warrants closer scrutiny: the information environment (or *infosphere*). While the information environment's existence is well documented in literature and joint military doctrine, the pressure of constant technological and geopolitical upheaval, a related tendency for wholesale acceptance of Information Age values, and historical experiences with fog and friction *have limited the US military's ability to truly appreciate the implications of operating within such an environment across a spectrum of conflict*.

At present, Information Age warfare is more distinguished by its conceptual underpinnings than any comprehensive change to war's nature, yet concerns arise over the challenges of gaining the advantage and controlling strategic outcomes in the twenty-first century. As strategists and theorists continue to determine what Information Age warfare entails, history provides an opportunity to interpret current events. Military theorists and strategists have sought information superiority over their adversaries since antiquity. Additionally, the importance of information in society and war has always existed, but its relationship varies. James Gleick, in speaking of the current paradigm,

clarified, "We see information in the foreground [today]. But it has always been there. It pervaded our ancestors' world, too, taking forms from solid to ethereal, granite gravestones and the whisper of courtiers."[31] Eliot Cohen's earlier commentary on a second communications revolution alluded to an enduring quality of society and war, appropriately phrasing his conclusion as a recurring reality: "the role played by that information in all of civilized life *will again transform society* and ultimately the conduct of war" (emphasis added). Not surprisingly, the enduring importance of information technology, its proliferation, and the fear of an inability to control it is not new. Consider Gleick's analysis of the alphabet, a distinct challenge for ancient rulers seeking to secure their interests (emphasis added):

> The alphabet is the most reductive, most subversive of all scripts…. The ruling priestly classes were invested in their writing systems. Whoever owned the scripts owned the laws and rites. *But self-preservation had to compete with [mankind's] desire for rapid communication*…. The alphabet spread by contagion. The new technology was both the virus and the vector of transmission. *It could not be monopolized, and it could not be suppressed*.[32]

Most importantly, what made the alphabet work was a medium for capturing the symbols—papyrus, dirt, granite, etc. The promulgation of the written word, whose meaning and relevance is granted only through cognition and perception, requires a platform for its effect. Moreover, preservation of the physical document remains crucial for message dissemination.

Here, the fundamental connection between the Industrial and Information Age emerges: *similar to the alphabet, globally distributed data today achieves its effect first through the existence of integrated information systems manufactured and distributed by industrialized societies*. As noted by the Institute for Defense Analyses (IDA), "Information Age technology is built on a strong industrial economy."[33] Thus, while Information Age mentality favors non-tangible solutions, their application relies on the existence of tangible products—the ability to choose and prioritize non-linear approaches implies a capability that enables one to do so. Previously mentioned attributes of mass

---

[31] Gleick, 12.
[32] Gleick, 33-34.
[33] Rothrock et al., 4.

and rapid communication, distribution, access, consumption, and collaboration are made possible first through the proper integration and employment of physical information systems. A dangerous condition arrives when such effects are assumed and their underlying enablers are no longer prioritized or even identified. Therefore, as a starting point for transformation, if the US defense establishment values Information Age precepts and seeks to exploit their benefits in war, Information Age strategists must continue to attribute worth to the physical platforms that enable information-centric effects.

In a broader sense, Industrial and Information Age qualities are connected through the confines of human nature, and hence war's nature, as discussed in Chapter 1. David Lonsdale debunked a revolution in military affairs (RMA) assertion after Desert Storm by transposing Clausewitz's theory of war to the present day. Lonsdale submits, "The nature of war is [*sic*] molded by . . . the policy objective, geography, the polymorphous character of war, the paradoxical logic and the fact that war is an activity waged by humans."[34] The same factors influence war in the present age, and the fundamental role of violence (or the threat of violence), purported by Clausewitz, underscores each element.[35] In the same way, J.C. Wylie codified war's purpose as obtaining some measure of control over an adversary. Wylie further highlighted an aspect of war and control that transcends any paradigm and represents an enduring reality of conflict: "*The ultimate determinant in war is the man on the scene with the gun* . . . if the strategist is forced to strive for final and ultimate control, he must establish, or must present as an inevitable prospect, a man on the scene with a gun" (emphasis in original).[36]

Thus, in the pursuit of finding differences that matter—or manageable differences in a methodical transformation—how the man with a gun *arrives* at the scene and subsequently *applies* his weapon provides the link that both connects and differentiates

[34] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*, (New York, NY: Frank Cass, 2004), 230.
[35] This idea runs contrary to some RMA theorists who suggested Information Age warfare would remove the need for violence and instead placed decisive victory in the attainment of information dominance. In direct contrast, Clausewitz established violence as the rudimentary force in war: "The fact that slaughter is a horrifying spectacle must make us take war more seriously, but not provide an excuse for gradually blunting our swords in the name of humanity. Sooner or later someone will come along with a sharp sword and hack off our arms." See Lonsdale, 230.
[36] J.C. Wylie, *Military Strategy: A General Theory of Power Control*, (Annapolis, MD: Naval Institute Press, 1967), 72.

Industrial Age and Information Age warfare. Imagine a soldier in the Napoleonic armies of Europe, equipped with the available weaponry of his time, fighting alongside his brethren in standard formation. His world and his war are right in front of him, and his commander's world extends across the horizon, but they rarely interact. His rifle is an extension of his body, employed by nothing more than his physical strength and acumen—the soldier, his rifle, and his unit achieve their effects through brute strength and their commander's cunning prior to battle.[37] That same soldier, transplanted through time, functions in an increasingly complex world and an equally complex war, as railroads, telegraphs, breech loading rifles, airplanes, radios, and radar systems all extend the battlefield, augment his physical skills, and place him in virtual contact with his commander and brothers in arms around the world. Eventually, the soldier, now in coordination with his fellow airmen, seaman, and marines, directs highly sophisticated and networked machines across air, land, and sea, synchronized through a web of intricate communication architectures traversing space and the EMS. His new weapons are capable of reaching anywhere in the globe at a moment's notice with unmistakable precision but are increasingly reliant on the availability of communication networks for their functionality. Similarly, his commanders now direct forces halfway across the world from their C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) centers, connected by the same communication architectures that empower the weapon systems that deliver their desired effects.[38] His warfighting units are smaller, less homogenous, and more dispersed, and he calculates firepower as a relative aggregate rather than a zero-sum quantity.

While somewhat dramatic, this visualization captures the essence of what has discreetly transpired over the last century. The warfighter is increasingly connected with information, and the weapons he employs function in a world that is only partially his

[37] In conventional war, the degree of violence employed by the soldier (its selectiveness) was tied to available information—the less information available, the more indiscriminate the violence. His organization was built on the premise that mass destruction was a solution to fog and friction imposed in part by informational deficiencies. Therefore, a lack of information did not necessarily prevent him from accomplishing the task at hand, and protection of information sources remained secondary, relative to the defeat of enemy forces.

[38] C4ISR is a broader, more holistic description of traditional C2 functions. See Jeffrey M. Reilly, *Operational Design: Distilling Clarity from Complexity for Decisive Action*, (Maxwell Air Force Base, AL: Air University Press, 2012), 63-64.

own. The industrial society, fueled by a voracious desire for more information, was finally able to create systems that could address the demand signal. In the process, a new environment that is part physical, part virtual, and part conceptual materialized around the warfighter (unbeknownst to him): information environments, or infospheres—virtual and physical realms that encompass, circumscribe, and energize human actions. The environments grew out of an industrial society and enabled the realization of Information Age capabilities, inadvertently forming the essential framework for national prosperity and national security (i.e., force projection and force application—the man's arrival on the scene and his use of the gun) in the twenty-first century. Evidence suggests that militaries do not fully understand or appreciate the strategic implications of infospheres and their relationship to achieving information control or information superiority. This is the result of historical experiences with unreliable or unavailable information and current experiences of operating within readily accessible and highly effective information environments.

Infospheres

The concept of an infosphere is not new. For over a decade, academic literature and military doctrine have alluded to its existence and remarked on its growing significance to national security. The US military defines the information environment as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."[39] However, the description is broad and generates undue levels of complexity for strategists to appropriately allocate resources and exploit its utility. From a slightly different perspective, David Lonsdale iterates a notion of "information power" that resides in its own strategic dimension, similar to its air, land, and sea power counterparts in their respective domains. Lonsdale refrains from offering a distinct definition of the amorphous environment, but offers a comparison in the way of a sea-lane or highway "through which information and weapons can flow."[40] David Alberts, John Garstka, Richard Hayes, and David Signori, contributors to the US Defense Department's Command and Control Research Program (CCRP), provide the most

---

[39] Joint Publication 3-13, *Information Operations*, 20 November 2014, ix.
[40] Lonsdale, 181.

utilitarian description of the information environment—henceforth referred to as the *infosphere* due to its more descriptive quality.[41] The analysts divide the environment into three parts, referred to as the physical, information, and cognitive domains.[42] To avoid confusion over terminology in subsequent chapters, the term *domain* in reference to an infosphere's structure is hereafter referred to as *dimension*.

To properly scope the remainder of the analysis, information control is primarily associated with the identification and preservation of *organic essentials*, or the physical and virtual information pathways upon which messages traverse. In this sense, information control does *not* refer to the manipulation or transmission of strategic messaging or narratives. As a result, the cognitive dimension—a critical element of the infosphere—falls outside of the basic concept of controlling access to the physical and information dimensions that collect and disseminate information for decision-making. Instead, the cognitive dimension serves as the source for prioritizing the establishment and protection of the physical and information dimensions to ensure infosphere accessibility in non-permissive environments.

Physical Dimension

Supplementary exploration of the three segments provides a useful framework for identifying and understanding the infosphere and how it relates to strategy. First, the physical dimension represents the portion "where physical platforms and the communications networks that connect them reside."[43] All aspects of information processing and exploitation rely first on capabilities in the physical realm (recall the example of the alphabet). Satellites, fiber optic cables, the EMS, computers, satellite ground terminals, modems, communication relay stations, other ISR (intelligence, surveillance, and reconnaissance) platforms, and humans comprise the physical

---

[41] In their 2001 report, *Understanding Information Age Warfare*, Alberts, Gartska, Hayes, and Signori refer to the information environment as the *infostructure*. For the purposes of this analysis, the term *information environment* is too broad to capture the true essence of the phenomenon and *infostructure* connotes a more physical and rigorous artifact that fails to describe its amorphous nature. *Infosphere* provides an all-around descriptor for the entity's encompassing characteristics, both in the physical and virtual realms.
[42] David S. Alberts, John J. Garstka, Richard E. Hayes, and David A. Signori, *Understanding Information Age Warfare*, (Washington, DC: DoD Command and Control Research Program), 11.
[43] Alberts et al., 12.

dimension and backbone of the infosphere.[44] In short, information collection and dissemination systems, discussed at length in Chapter 1, constitute the infosphere's physical dimension.

The infosphere is an enduring artifact from antiquity, but its physical dimension did not assume its encompassing form until the 1950s when exploitation of the space medium first occurred. Space operations, perhaps the ultimate bastion of an industrial society, redefined information collection and dissemination capabilities and inadvertently brought substance to Information Age concepts. As described earlier, the space architecture, consisting of ground and on-orbit segments coupled by the EMS, effectively fuses Industrial Age production with networked communications that drive functionality, a fundamental requirement for Industrial Age thinking. Furthermore, space architectures, extending within and beyond the earth's atmosphere, involve ground-to-satellite, satellite-to-satellite, and satellite-to-ground communications, enabling rapid, global collection and distribution of data and forming both a physical and virtual dome over human activity. For example, in 1965, INTELSAT 1, the product of an international consortium led by the United States, became the first global satellite communications network. Within just a few years, available telephone circuits increased from five hundred to several thousand and access to live television coverage around the world was suddenly considered routine. Indeed, "With this satellite system in orbit the world became a far different place."[45] In essence, space architectures established the initial foundation for a modern, global infosphere.

Most notably, space architectures, now coupled with cyberspace networks on earth, continue to serve as a foundational component of an infosphere's physical dimension. To once again refine the analysis, *cyberspace* is confined to "the realm of computer networks . . . in which information is stored, shared, and communicated online."[46] As such, cyberspace constitutes *ground-based* communication networks, providing an overlap but distinct demarcation with space. In this regard, while information systems include a wide variety of capabilities and technologies across all

[44] Lonsdale, 182.
[45] Roger D. Launius, *NASA: A History of the U.S. Civil Space Program*, (Malabar, FL: Krieger Publishing Company, 1994), 37.
[46] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, (New York, NY: Oxford University Press, 2014), 13.

domains (land, sea, air, space, and cyberspace), only space and cyberspace are exploited for the primary purpose of collecting and disseminating information on a global scale.[47] Each of the two domains proves integral to the whole, offering distinctive vantage points and accesses for information collection. Additionally, each domain complements the other within a collection-dissemination framework. For instance, on-orbit assets offer unique global, regional, and persistent coverage opportunities for a wide variety of data by exploiting extreme altitudes and collection technologies (operating across the entire EMS). Moreover, the process of collecting and disseminating data across the globe inevitably incorporates space- and terrestrial-based communication networks.

Nevertheless, close scrutiny of joint doctrine and operations reveals that of the two information-centric domains, only cyberspace is considered a dominant component of infospheres, with space relegated to peripheral support of information operations.[48] Service and domain parochialisms abound in Industrial Age thinking, as military organizations are distinguished by specific, predetermined tasks according to their assigned domains. Consequently, the concurrent emergence of cyberspace with the Information Age generated conceptual and traditional linkages that apportioned information-centric operations predominately to the cyberspace domain. As shown, cyberspace capabilities undoubtedly represent an output of the new era, but they are "only a part of the infosphere."[49] The prevailing mindset overlooks the fact that space architectures and missions ushered in the dawn of the Information Age and, alongside cyberspace, constitute equally important components of an infosphere's physical dimension. Thus, from a warfighting perspective, any notion of information control first depends upon the combined identification and protection of associated space and cyberspace systems in the physical dimension, prioritized by a particular strategy's information requirements.[50]

---

[47] For the purposes of this analysis, space and cyberspace systems form the backbone of an infosphere's physical dimension. Information systems that subsist within other domains—for example, airborne ISR platforms—constitute peripheral capabilities that insert themselves into the broader framework created by integrated space and cyberspace networks.

[48] Joint publications place primary focus on cyberspace operations as the cornerstone of information operations, while space doctrine articulates its role in information operations as secondary. This relationship is explored further in Chapter 3. See Joint Publication 3-13, *Information Operations*, 20 November 2014, II-6, II-9.; and Joint Publication 3-14, *Space Operations*, 29 May 2013, I-4.

[49] Lonsdale, 183.

[50] This connection underscores the principle discussion of the next chapter.

Information Dimension

The information dimension results from information collection in the physical dimension and represents the virtual component of an infosphere. Accordingly, the information dimension is "the [dimension] where information lives . . . where information is created, manipulated, and shared."[51] Military theorists that promote mental paralysis of the enemy (e.g., Sun Tzu, Liddell Hart, J.F.C. Fuller, and John Boyd) seek to manipulate the information dimension and view the dimension as "ground zero" in the pursuit of information superiority.[52] Despite this emphasis, CCRP analysts recognized the direct correlation between the information and physical dimensions:

> A sensor [in the physical dimension] observes the real world and produces an output (data), which exists in the information [dimension]. With the exception of direct sensory observation [which transmits data straight to the cognitive dimension], all of our information about the world comes through and is affected by our interaction with the information [dimension].[53]

Simplified, the information dimension contains the *virtual pathways* that contain messages observed and conveyed from the physical dimension—data points arranged in binary form (1s and 0s) and/or symbols (e.g., the alphabet) that ultimately infer meaning. These virtual pathways represent the organic essentials necessary for making decisions and taking action. In this sense, the CCRP analysts conclude that protection of the information dimension constitutes the highest priority, but a slightly alternate view distinguishes the information dimension as the realm that *drives the protection of the infosphere as an entity*, which begins with the physical dimension. Figure 3 presents a basic diagram of the backbone that defines an infosphere's physical and information dimensions (characterized by global, near instantaneous, and accessible information collection and dissemination).

---

51 Alberts et al., 12.
52 Alberts et al., 13.
53 Alberts et al., 12.

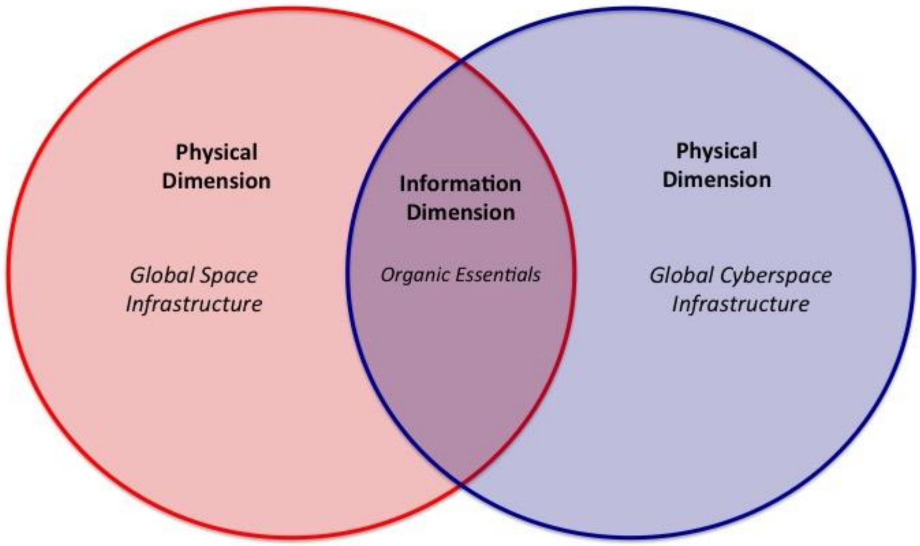

Figure 3: The Backbone of an Infosphere's Physical and Information Dimensions
Source: Author's Original Work

Cognitive Dimension

A message's relevance and meaning, however, do not exist without interpretation. Hence, the cognitive dimension includes the requesters, users, and interpreters of information. As noted, the cognitive dimension is not directly associated with actions to obtain information control, however.[54] Rather, *the cognitive dimension sets information requirements by attributing relevance and meaning to the data collected*, thus representing the driving force behind the infosphere's utility and prioritization. The dimension exists "in the minds of the participants . . . where perceptions, awareness, understanding, beliefs, and values reside and where . . . decisions are made."[55] The cognitive dimension is the battleground for information operations and the arena where psychological paralysis takes place. Manipulation of the information dimension affects

[54] The subjectivity of cognition prevents the establishment of a consistent model for information control. Indeed, "Prejudices, preconceptions, and personal experience cause similarly situated commanders to read the same information differently." Reference Jurgen Brauer and Hubert Van Tuyll, *Castles, Battles, and Bombs: How Economics Explains Military History*, (Chicago, IL: The University of Chicago Press, 2008), 195. Therefore, information control is concerned with the preservation of information collection and dissemination systems that enable cognitive processing, decision-making, and action.
[55] Alberts et al., 13.

deduction and conclusions formed in the cognitive dimension, leading to decisions and resultant actions that may otherwise not transpire. Therefore, interpretation and directed action—the true purpose of information gathering—occur in the infosphere's cognitive dimension.

Proliferation of information systems in the physical dimension and the information dimension's resultant expansion has altered the cognitive dimension's traditional definition. Historically, the cognitive dimension resided exclusively in the human mind. The commander's ability to filter relevant information and direct his forces through uncertainty constituted the essence of Clausewitz's military genius. The concept of military genius exists today, and continues to form the basis of strategy, as examined in Chapter 1. However, the availability and preponderance of networked information systems eventually led to the development and employment of net-centric C4ISR and weapon systems reliant on infospheres for their functionality. Command systems such as the air and space operations center (AOC) are designed to operate with and filter incredible amounts if information—their effectiveness (if not their basic operation) is infosphere-dependent. Other examples include fifth-generation fighters (i.e., the F-22 and F-35) and ballistic missile characterization and warning systems, all of which process and rely on externally collected and distributed information to produce intended effects. As a result, the human mind no longer signifies the sole interpreter of data that assigns meaning and relevance to information; *in the Information Age, net-centric machines also comprise the cognitive dimension*. In the end, Information Age warfare is characterized by the mutual functions of man and machine—decision-making and delivery of effects—that depend on the infosphere for their fulfillment. In this context, *information control starts with the protection of the physical and information dimensions that collect and disseminate data for interpretation in the cognitive dimension*.

Key Characteristics of Infospheres

In essence, global infospheres do exist, incorporating the whole of information collection and distribution systems in space and cyberspace and the resultant information pathways. However, infospheres are man-made phenomena that are scalable and malleable (*and not inevitable*). Moreover, multiple infospheres can and do exist

simultaneously, both independent of and interdependent with one another (by virtue of the global space and cyberspace architecture).[56] In this regard, infospheres subsist as global and regional entities, enabling and connecting enduring operations with ad hoc events.

Identification and formation of an infosphere is situation dependent *and is formed around operational necessity* (congruent with the desired strategy). Infospheres are set up, torn down, and adjusted as required. On a global scale, steady state or strategic infospheres serve long-standing national (and international) activities, remaining relatively consistent and robust in their function and design. On a regional scale, secondary infospheres rise and fall in support of regional or theater crises. These contingency infospheres are more dynamic and flexible, tailored to specific and emerging informational needs, and may form as offshoots of the established strategic infospheres that govern long-standing operations. For instance, as information and mission requirements develop or change, additional systems and networks (e.g., satellites and satellite constellations, land lines, collaborative environments, ISR assets), may enter or withdraw from the environment or collect and disseminate different information based on anticipated or ad-hoc decision points, force projection considerations, and force employment. Consequently, theater infospheres potentially incorporate competing space and cyberspace resources from the strategic (global) environment as well as other regional infospheres, but may also use local resources, particularly in cyberspace, which subsequently connect to strategic infospheres. By definition, then, infospheres are scalable, assembled to support long-term global requirements, theater campaign plans, campaign operations, specific missions, single units, and even individual warfighters or weapon systems. In fact, any campaign effort will involve multiple (possibly hundreds) infospheres integrated and coordinated in direct and indirect support of its planning, execution, and assessment.

Needless to say, a clear delineation does not exist between infospheres, creating a convoluted challenge for strategists to overcome. Additionally, the Information Age has matured in a unipolar and permissive environment, allowing US strategists to overlook some of the intricacies inherent in the networked infrastructures that facilitated dominant

[56] Lonsdale, 183.

force projection and application efforts since Desert Storm. As state and non-state actors rise on the international scene, the default advantages enjoyed by US forces are quickly eroding, placing greater impetus on sound strategic analysis of information control and superiority. Regardless of the era, strategists have always attempted to define the environments within which they operate to understand their implications and secure access for eventual influence or control. The infosphere is no different in this regard, yet its relationship to national and military strategy has thus far been difficult to qualify.

Implications for Strategy

The infosphere undoubtedly creates significant complications for strategists to consider. In fact, its complexity is such that its creation, identification, prioritization, management, protection, and exploitation demand a higher level of effort and resourcing than currently allocated. The physical dimension alone incorporates systems with a wide range of capabilities and support networks, and its backbone constitutes national level enterprises in space and cyberspace that traditionally lack a unifying imperative for integration. Furthermore, the unique environment that defined the post Cold War era gave the rest of the world a singular focus for their defense efforts, while the United States developed strategies to counter a broad spectrum of tenuous threats. By planning and operating with technological supremacy, the US military freely accepted a highly sophisticated information architecture that bolstered its expectations for success and became a "logical target for the enemy," one that "must be most vigilantly protected."[57] Lonsdale expresses the infosphere's true extent in modern strategy in what he considers a fifth dimension in war:

> The rise in the significance of the infosphere . . . cannot be ignored. Strategy in the infosphere has its own character, and requires operations, organizations and career paths that are specific to its unique nature. The dominant operational and strategic concept in this fifth dimension is 'control of the infosphere.'[58]

The loss of access to the infosphere can severely disrupt an industrialized society's desired way of life and even neutralize a military's desired way of war in the twenty-first

---

[57] Martin Libicki and Jeremy Shapiro, *The Changing Role of Information in Warfare*, (RAND: Project Air Force, 1999), 439.
[58] Lonsdale, 214.

century (forcing decision makers to choose between a range of options that include reverting to mass warfare—involving more indiscriminate violence—or ceasing hostilities altogether). Thus, identifying and controlling access to infospheres can ensure preservation of societal and military priorities and constitutes a fundamental necessity in Information Age warfare (see Figure 4). Controlling one's respective infospheres requires the comprehensive development of offensive and defensive campaigns and capabilities, cornerstones of control operations.

A connection between the identification and protection of the infosphere, information warfare, information control, and information superiority in the twenty-first century now emerges. In essence, the ability to define and secure one's infosphere (beginning in the physical dimension and prioritized by the information and cognitive dimension) creates conditions whereby forces can control access to the information they need (by way of securing freedom of access and maneuverability for collection and dissemination in the physical domain) to make decisions, take actions, and achieve objectives. Because the infosphere grows from the integration of space and cyberspace capabilities, information control initiates with sufficient and integrated control of the space and cyberspace domains, paving the way for a relative advantage in the attainment of information superiority. Accordingly, an investigation on how the joint force can incorporate these concepts into military strategy follows. The enduring premises outlined in Chapter 1 provides context for such an endeavor: the critical balance between strategy, decision-making, and information.

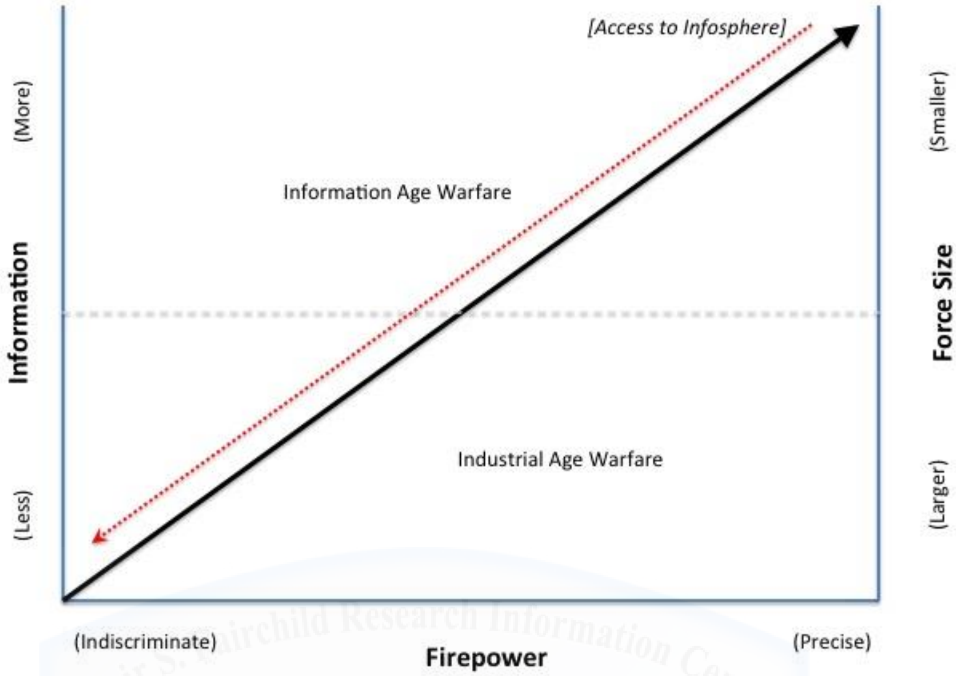

Figure 4: Access to the Infosphere and its Relationship to Force Employment
Source: Author's Original Work

Conclusion

Organizations tend to avoid uncertainty and change, and the US military is no exception. The advent of the Information Age and its disruptive concepts appear to challenge traditional paradigms, creating anxiety in some defense bureaucracies. In reality, the Information Age has indeed marshaled in a new way of war, but it has not redefined it. War involves decision-making supported or influenced by information (or a lack thereof), and hence the value of accurate, timely information for decision-making endures. It is therefore no surprise that the Information Age—characterized by global, near instantaneous, and accessible information collection and dissemination—eventually emerged. However, its existence was recognized long after its origin, affecting the US military's ability to properly align itself with the new landscape. Fortunately, opportunities for transformation in the new era exist, rooted in the reclassification of an Industrial Age product that sparked Information Age thinking: the modern infosphere,

whose backbone is comprised of space and cyberspace platforms and networks and the information they collect and disseminate

The materialization of infospheres *has* changed the importance of information from a C2 and warfighting capability perspective, however, highlighting a potential bridge between Industrial Age and Information Age warfare. While humans have historically operated with limited information and uncertainty during war (i.e., military genius), the systems they now procure, project, and employ across the globe automatically assume the availability of sophisticated information networks, demanding the sustainment and protection of the infosphere to function properly (or at all). Notably, control of the infosphere first requires identification and protection of prioritized assets in the physical dimension (i.e., space and cyberspace) that collect and disseminate requisite information—denoting a traditional viewpoint of war in support of a new paradigm.[59] Control of the infosphere in this manner indicates a first step in redefining information control and information superiority in the twenty-first century. Furthermore, the connections between controlling global and/or theater infospheres (via coordinated and integrated control of space and cyberspace), and information control exist in the long-standing relationship between strategy, decision-making, and information writ large.

Ultimately, by continuing to structure itself along traditional perspectives of warfare while exploiting advanced information technologies against increasingly limited resistance, the US military finds itself in a position where it is not fully optimized for the demands of Information Age warfare. As a result, a paradigm shift is needed to acknowledge the criticality of infospheres on force projection and application, particularly if the US military intends to preserve its desired way of war. Subsequently, the US military must reevaluate its current structure and concepts of operation to determine their utility in future wars. In broad terms, a paradigm shift manifests itself in the acceptance of a comprehensive and prioritized information control strategy centered on the identification and protection of infospheres. In this regard, the analysis continues in Chapter 3 with a detailed examination of how the theoretical concepts described thus far may influence current and future joint operations.

[59] Industrial Age warfare places higher value on the protection of physical platforms while Information Age warfare values the collective capabilities they produce.

Chapter 3

Implications for the Joint Force—New Strategic and Operational Imperatives

That vast organizations, as well as billions of dollars in equipment, are necessary to make [a telephone] call possible at all is something of which most of us are only dimly aware.

- Martin Van Creveld

In national wars of the second half of the nineteenth century, two eras of military art and two military schools were, in essence, struggling. Predominance, of course, went to the one which took into account the new conditions of its time.

- G. Isserson

The character and form assumed by the war of the future is the fundamental basis upon which depends what dispositions of the means of war will provide a really effective defense of the state.

- Guilio Douhet

We thus obtain three requirements to control: information, decision, and communication, the third being the cooperative link between the first and second and the expenditure of fighting force.

- J.F.C. Fuller

The dominant operational and strategic concept in this fifth dimension is 'control of the infosphere.'

- David Lonsdale

The United States and its military reap the asymmetrical benefits afforded by global information networks. National prosperity and national security not only rely but also depend on information systems for their sustainment. From a national security standpoint, the maturation of infospheres directly enabled the delivery of rapid, worldwide, lean, concentrated, and precise lethality using globally dispersed and traditionally disparate capabilities. From a great power perspective, the development and proliferation of information systems in a relatively benign strategic environment created a situation in which the US economy and defense apparatus incorporated new technologies with little external resistance or clear threats. The communication infrastructures built during the Industrial Age could suddenly flourish, relatively unchecked, producing collaborative experiences that perpetuated the dynamic values of the Information Age. Consequently, new expectations of force projection and force employment grew from notions of net-centricity and redefined the US desired way of war, characterized by the traits listed above. In essence, *all national and military activities now subsist under the physical and virtual domes of globally connected infospheres, comprised of the*

interdependent network of space and cyberspace systems. Now, in a time of great technological and geopolitical change, US strategists must understand the potential capabilities, limitations, and susceptibilities inherent in their desired way of war, particularly as near-peer adversaries continue to develop methods for neutralizing previous information advantages.

Various national and joint publications articulate a growing sentiment for the criticality of information systems to national prosperity and security. For example, Joint Publication (JP) 3-12, *Cyberspace Operations*, states, “The prosperity and security of our nation have been significantly enhanced by our use of cyberspace, yet these same developments have led to increased vulnerabilities and a critical dependence on cyberspace, for the United States in general and the joint force in particular.”[1] In a similar vein, JP 3-14, *Space Operations*, reads, “Military, civil, and commercial sectors of the US are increasingly dependent on space capabilities, and this dependence is a potential vulnerability as space becomes increasingly congested, contested, and competitive.”[2] Likewise, the 2011 National Security Space Strategy (NSSS) claims, “Space is vital to U.S. national security and our ability to understand emerging threats, project power globally, conduct operations, support diplomatic efforts, and enable global economic viability.”[3] Joint Publication 3-13, *Information Operations*, further establishes the guidelines for manipulating adversary decision-making processes and protecting one’s own by exploiting information related capabilities (IRC).[4] Space and cyberspace systems now comprise the backbone of national prosperity and security and provide decision-makers options for gaining asymmetric advantages in modern warfare.

Viewed holistically, these examples express the underpinnings of an evolving strategic requirement. If the United States seeks to preserve its way of life (prosperity) and desired way of warfare (security), then it must recognize the enabling factors that create the preferred conditions and deliberately secure them. History suggests that he who controls access to *relevant* information can experience a decided advantage over an opponent. In the Information Age, that access is gained first through the identification,

---

[1] Joint Publication 3-12(R), *Cyberspace Operations*, 5 February 2013, v.
[2] Joint Publication 3-14, *Space Operations*, 29 May 2013, I-2.
[3] US Department of Defense, *National Security Space Strategy*, (Washington, DC: Office of the Secretary of Defense, 2011), 1.
[4] Joint Publication 3-13, *Information Operations*, 20 November 2014, ix.

protection, and control of the respective infospheres supporting one's enacted strategy, campaign, operation, and/or mission.

An investigation on how the joint force can begin identifying and securing the infospheres that support its strategies comes to the fore. The approach is certainly not comprehensive, and additional analyses are necessary, but it serves as a point of departure for rethinking prevailing strategies (and assumptions) for force projection and force employment in future conflicts. To this end, the chapter is divided into three sections. The first section provides context by discussing conventional methods of strategy development, domain control, awareness of the operational environment, and decision-making at the campaign level. The second section proposes a new paradigm that redefines and prioritizes information control as an overarching strategy for war, manifested first through controlled access to infospheres. In this sense, the complexities associated with identifying and securing access to an infosphere demand a broader set of resources and authorities than are currently allocated. Under the new paradigm, information control warrants its own unified strategy—at least proportionate with traditional campaign-level efforts—distinct from, yet integrated with, global and theater operations. Finally, the chapter summarizes potential shortfalls in current joint doctrine and other operational perspectives that may limit the attainment of the proposed Information Age warfare requirements and, most significantly, the preservation of America's desired way of warfare.

Strategy, Decision-Making, and Information Revisited

Before proceeding, a brief review of the timeless relationship between strategy, decision-making, and information presented in Chapter 1 provides necessary context for subsequent analyses. Strategy serves as a methodology for gaining an advantage and leveraging control over a situation to project or secure interests. It fulfills basic elements of human interaction (i.e., competition) by addressing the fundamental fear of an inability to shape outcomes corresponding to one's desires. An evolving process, sound strategy never ends and seeks to anticipate the next steps in relation to the dynamic environments within which it functions. However, anticipation alone only sets expectations and does not provide direction for action. Taking action requires some form of decision-making,

and thus a robust strategy identifies decision authorities and incorporates respective decision-making opportunities—both anticipated and ad-hoc—into its subordinate plans.

Relevant information represents the binding agent for strategy, decision-making, action, and success. Strategy builds the context for anticipation, decisions, and actions, which demand a certain amount of information for cognitive processing. Thus, strategy establishes prioritized information requirements to support its development and execution. This prioritization allows national leaders, military commanders, planning staffs, warfighting units, and individual combatants or systems to filter irrelevant data and respond in *accordance with a particular strategy's intent*. As highlighted in Chapter 1, the capability to acquire vast amounts of information does not necessarily create an impetus to do so, nor does a greater availability of information automatically translate to success. An abundance of information, or data, without an effective strategy or associated decision points is nothing more than a burden, if not a disadvantage.

The challenge for strategists, then—particularly in the Information Age—is to retain strategy's primacy in war and extract informational needs within its framework rather than assuming vast quantities of information will invariably lead to more robust operations.[5] Moreover, prioritized information requirements enable strategy employment, and therefore the loss of access to said information could prove detrimental. Just as significantly, the loss of requisite information may limit a force's ability to anticipate or adapt to fluctuations in its operating environment. Consequently, strategists must place great emphasis on identifying and securing access to the infospheres (including the physical, information, and cognitive realms) that enable their strategy's effectiveness.

Conventional Methods of Military Strategy and Planning

Strategy exists at multiple levels and, if done correctly, best functions within a hierarchical structure. At the top, grand strategy articulates broad, sweeping guidance and prioritized objectives for the state. Grand strategy provides a general framework for

[5] Appreciating the relationship between strategy, decision-making, and information also provides a means for reducing anxiety in a rapidly changing environment. While information systems abound, and information saturation consumes decision-makers, commanders still have the ability to manage their informational requirements based on the strategy they employ.

unifying and mobilizing sources of national power (i.e., diplomatic, economic, information, and military) to preserve and/or promote national interests, all of which are derived from deeply rooted values within the state's cultural base.[6] In the United States, departmental strategies—such as the National Defense Strategy (NDS)—subsequently flow from grand strategy. The NDS specifies defense objectives and priorities in support of grand strategy, and generates additional levels of strategic fidelity in the form of the National Military Strategy (NMS), Guidance for Employment of the Force (GEF), and the Joint Strategic Capabilities Plan (JSCP).[7] Thus, grand strategy, the NDS, NMS, GEF and JSCP provide the overarching basis for US military operations around the globe.

Strategists at lower levels develop regional plans based on the encompassing strategies mentioned above. For example, issued by the Secretary of Defense and approved by the president, the GEF purposely converts the National Defense Strategy's guidance into prioritized strategic objectives and communicates the global defense posture, which ultimately facilitates combatant command (CCMD) deliberate planning for their respective theater campaigns.[8] The Chairman of the Joint Chiefs of Staff (CJCS) works concurrently to produce the JSCP from the NMS, illustrating *how* the military will achieve the objectives conveyed in the GEF.[9] Specifically, the JSCP provides expectations to planners by indicating the level of planning required for each campaign plan and correspondingly apportions forces to that end. It also expresses military and operational guidance to combatant commanders (CCDR) as they conduct planning using

---

[6] The National Security Strategy (NSS) and Unified Command Plan (UCP) form the basis of US grand strategy. The NSS does not offer the DOD any direction on its roles in achieving its objectives. Therefore, as Commander in Chief of the Armed Forces, the president reveals and aligns US military warfighting organizational structures and responsibilities in the UCP, congruent with the strategic direction outlined in the NSS. Of note, the NSS codifies US interests on both a national and global scale, requiring US leadership well beyond its borders. To accommodate this daunting task, the UCP establishes Combatant Commands (CCMD) and divides their responsibilities based on region and function, consequently instituting a joint force command (JFC) construct. For additional details, reference: 1) Joint Staff, J7 JETD, Joint Officer Handbook (JOH), Staffing and Action Guide, 2d Ed., August 2011, 133. and 2) Andrew Feickert, *The Unified Command Plan and Combatant Commands: Background and Issues for Congress*, (Washington, DC: Congressional Research Service, 2013), 1.

[7] JP 1-0, *Doctrine for the Armed Forces of the United States*, 25 March 2013, II-4.; Joint Staff, J7 JETD, Joint Officer Handbook (JOH), Staffing and Action Guide, 2d Ed., August 2011, 132-133.

[8] Joint Staff, J7 JETD, Joint Officer Handbook (JOH), Staffing and Action Guide, 2d Ed., August 2011, 132.

[9] Patrick C. Sweeney, *A Primer for: Guidance for the Employment of Force (GEF), Joint Strategic Capabilities Plan (JSCP), the Adaptive Planning and Execution (APEX) System and Global Force Management (GFM),* (Providence, RI: Naval War College, 2011), 2.

existing military capabilities.[10] While grand strategy builds the overall framework for joint force command (JFC) authorities and planning priorities, the NDS, NMS, GEF, and JSCP present increasingly actionable, defense-centric guidance for JFC planning efforts. The GEF and JSCP task CCDRs and JFCs to generate executable, comprehensive campaign plans that integrate and synchronize joint forces to achieve military and national objectives within their respective combatant command.[11] The bevy of strategic documents set the stage for theater-level planning by providing "purpose and focus to the planning for employment of military force."[12]

For the purposes of this analysis, all references to military strategy and joint force doctrine in this chapter will henceforth remain at the campaign level (combatant command) or below, unless otherwise noted. According to Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, a campaign is "a series of related major operations aimed at achieving strategic and operational objectives within a given time and space."[13] Furthermore, Joint Publication 5-0, *Joint Operation Planning*, indicates "campaigns are often the most extensive joint operations in terms of time and other resources" and "campaign planning has its greatest application in the conduct of large-scale combat operations, but can be used across the range of military operations."[14] As expected, campaign plans codify strategies at the theater level and therefore strive to balance associated strategic intent, decision-making opportunities, and informational requirements in their calculus.

The Role of Domain Control and Superiority in Military Operations

Investigating how and why combatant commanders organize their forces, prioritize efforts, delineate roles and responsibilities, and direct actions within their campaigns reveals symptoms of a larger paradigm. First, military operations—like any other competitive human endeavor—exist to gain an advantage and exert some level of control over the enemy or situation. To this end, and to achieve greater effectiveness across the joint force, traditional military strategies and plans demarcate spatial and

---

[10] JP 5-0, *Joint Operational Planning*, 11 August 2011, II-6.
[11] Sweeney, 7.
[12] JP 5-0, I-2.
[13] JP 1-02, 27.
[14] JP 5-0, II-21, II-22.

temporal requirements for control. In other words, strategy circumscribes the operational environment and dictates where control is needed, when it is needed, and its required duration.

The concept of control—and its heir apparent, *superiority*—drives military force structures, responsibilities, and efforts. Joint forces plan and conduct operations in and through several mediums, including land, sea, air, space and cyberspace, and the Defense Department delineates service roles and responsibilities accordingly. From a spatial standpoint, control of an operational environment is attained through assured and sustained access to the mediums within which military operations occur, which first implies a certain level of *presence*. These mediums—separated largely by their differing approaches to maneuvers, fires, and logistics—are categorized as domains, or conceptual structures that enable more effective planning and execution in complex environments. *Domains, then, serve as actionable and measurable targets for control*.

Notably, military strategists typically equate domain control with gaining and maintaining *domain superiority*, defined as a level of dominance in a particular medium "that permits the conduct of joint operations without effective opposition or prohibitive interference."[15] Therefore, depending on strategic requirements, campaign plans include objectives related to gaining and maintaining land, maritime, air, space, and/or cyberspace superiority as a way of securing control of a particular operational environment. The collective attainment of superiority across all applicable domains—known as *full-spectrum superiority*—is considered a key condition for gaining an advantage over the adversary and subsequently controlling strategic and/or political outcomes.[16]

Full-spectrum superiority facilitates force projection and employment through cross-domain operations, a key force multiplier and a critical utility for modern combat. As shown in Chapter 2, the prevalence of information technologies allows for collaboration and coordination across previously disparate operations, generating asymmetrical effects with exacting precision and minimal force. Military strategies and the national strategies they support now rely on the ability to seamlessly maneuver

[15] JP 1-02, 100.
[16] JP 1-02, 100.

between domains and apply lethal (or non-lethal) force through multiple attack vectors. The anticipated result is a cascade of insurmountable firepower and pressure to paralyze enemy forces and decision makers.

Nevertheless, service and joint forces remain affiliated with specific domain designations, a remnant of traditional warfare that delineates roles and responsibilities and provides flexible options for statesmen and commanders. Each domain falls under the respective purview of the Army (land), Navy and Marine Corps (sea and land), and Air Force (air, space, and cyberspace). By design, each service provides expertise on how their forces can exploit its assigned domain(s) to achieve strategic objectives. As forces are brought to bear in a specific theater to support a combatant command's campaign, the joint force commander (JFC)—or combatant commander (CCDR)—typically assigns authorities and responsibilities using a *domain-centric* construct. Structurally, JFCs may align their forces under the guise of service or joint force (functional) component commands. Operationally, these component commands—whether service or joint—are primarily compartmentalized by warfighting domain (see Figure 5) and consist of service or joint capabilities associated with respective domain operations.[17] Accordingly, theater component commanders are responsible for gaining and maintaining domain superiority, both spatially and temporally, in accordance with campaign requirements. For example, air component commanders (e.g., the theater Commander of Air Force Forces [COMAFFOR] and/or Joint Forces Air Component Commander [JFACC]) are commonly tasked with coordinating, gaining, and maintaining air and space superiority in the JFC's AOR, as required.[18]

---

[17] JP 3-0, *Joint Operations*, 11 August 2011, IV-8. Of note, space and cyberspace are considered global domains and do not fall under the direct authority of a theater JFC, a key peculiarity examined later.

[18] The alignment of space operations with air power originates from a long-standing institutional belief that, like air, space is a physical domain extending from the earth's surface. For example, in November 1957, General Thomas White, then Chief of Staff of the USAF, remarked, "In speaking of the control of air and the control of space, I want to stress that there is no division, per se, between air and space. Air and space are an indivisible field of operations." Reference Donald Cox and Michael Stoiko, *Spacepower: What It Means to You*, (Philadelphia, PA: The John C. Winston Company, 1958), 122.

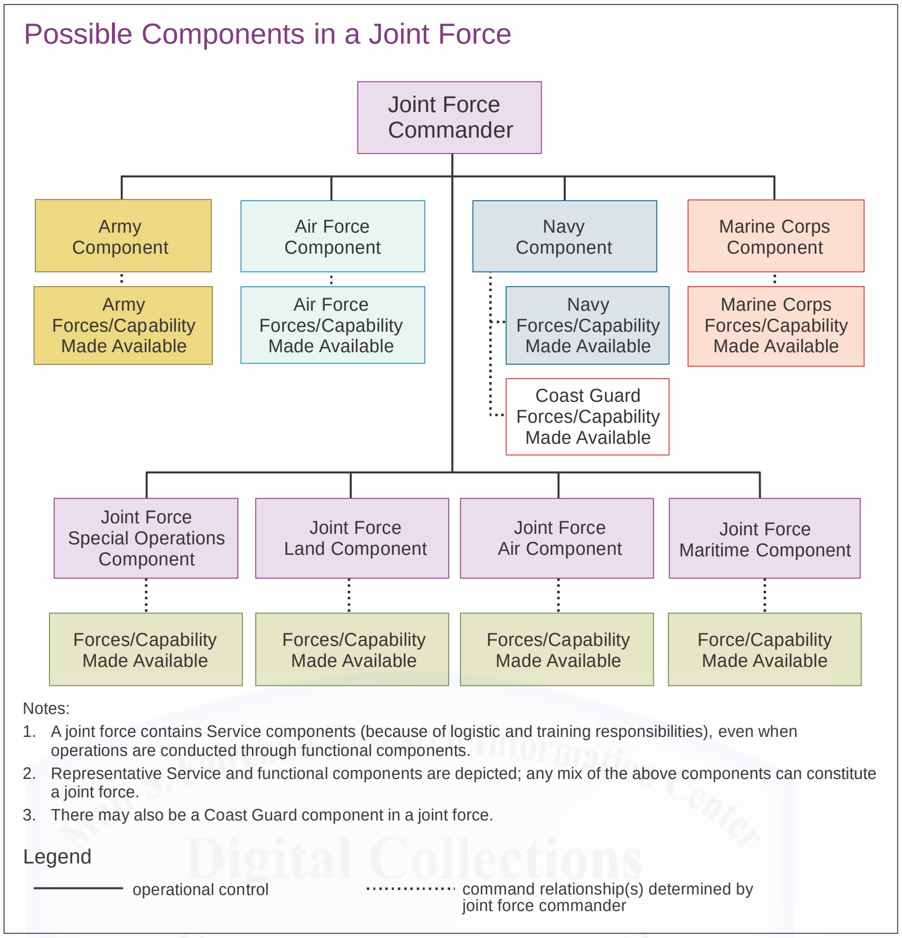

Figure 5: Possible Components of a Joint Force
Source: JP 1, Doctrine for the Armed Forces of the United States, 25 March 2013, IV-3.

Although service and joint forces are primarily compartmentalized by domain, domain operations are increasingly interdependent for achieving objectives. Current doctrine differentiates the domains between physical (land, maritime, air, and space) and primarily virtual (cyberspace) realms.[19] Land power, designed to control or contest territory, relies on air operations (and maritime shore operations) to enable or enhance their freedom of maneuver. Maritime power employs air and surface capabilities to control and/or contest access to sea lines of communication. Similarly, air power, capable of rapidly projecting force around the globe, functions to control access to air space and is increasingly viewed as a critical enabler for terrestrial-based operations. John Warden III, initial architect of the air component's immensely successful strategy during Operation Desert Storm in 1991, believed that possession of air superiority "is

[19] JP 3-12(R), I-2.

needed before other actions on the ground or in the air can be undertaken" and observed that "attainment of air superiority consistently has been a prelude to military victory."[20] The current Air Force Chief of Staff, General Mark A. Welsh III, amplified this belief when he remarked on social media, "Air power . . . because without it you lose."[21] Space power, while more politically volatile than its counterparts, delivers assured access to the space domain—the details of which are covered in Chapters 4 and 5. Finally, cyberspace, currently defined by the Defense Department as "a global domain within the information environment . . . [that] consists of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers," is currently viewed as the primary domain for information operations, discussed in detail later.[22] Thus, while interdependent, control of each domain offers unique advantages for strategists to exploit. The true value of any domain operation is determined by the approved strategy, which is informed through an in-depth understanding of the operational environment.

Understanding the Operational Environment

Strategy, as Sun Tzu professed, seeks to undermine an opponent's strategy to secure situational control. Correspondingly, Sun Tzu, and later Clausewitz, recognized the importance of surveying strategic and operational landscapes to appreciate the factors giving rise to and influencing a particular war.[23] Only then could politicians and commanders adequately assess their strategic intent, objectives, priorities, opportunities, and challenges, and develop an appropriate way ahead. At the campaign level, modern planning processes capture this activity in the joint intelligence preparation of the operating environment, or JIPOE. Joint Publication 3-0, *Joint Operations*, describes the

---

[20] John Andreas Olsen, *John Warden and the Renaissance of American Air Power*, (Washington, DC: Potomac Books, Inc., 2007), 66-67.

[21] General Mark A. Welsh III, *Global Vigilance, Global Reach, Global Power for America*, United States Air Force, 22 Aug 2013; 2 min., 5 sec. https://www.youtube.com/watch?v=ZvWkNGr8RiQ (accessed 21 March 2015). The general's comment encompasses the full spectrum of air power in the form of air, space, and cyberspace operations.

[22] JP 3-0, IV-2.

[23] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (London: Oxford University Press, 1963), 63.; Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 88.

operational environment below (note the distinction between space and cyberspace domains—an issue scrutinized later in this chapter):

> The JFC's operational environment is the composite of the conditions, circumstances, and influences that affect employment of capabilities and bear on the decisions of the commander. It encompasses physical areas and factors (of the air, land, maritime, and space domains) and the information environment (which includes cyberspace). Included within these are enemy, friendly, and neutral systems that are relevant to a specific joint operation. The nature and interaction of these systems will affect how the commander plans, organizes for, and conducts joint operations.[24]

Intelligence preparation efforts allow commanders and their planning staffs to frame the operational environment through the investigation of political, military, economic, social, information, and infrastructure (PMESII) considerations. Similarly, characterization of the operational environment provides a baseline for determining levels of control or superiority required across each domain. The entirety of the operational environment, while extending beyond the JFC's assigned area of responsibility (AOR), establishes physical margins for a domain's spatial focus (e.g., geographical boundaries, air space, and maritime boundaries) and compares related enemy intentions in the same areas.[25] In so doing, commanders build a composite portrait of the landscape that shapes strategy development and offers opportunities and challenges to strategy employment.

While designating a JFC's AOR and describing the operational environment help develop strategic and operational requirements for each domain, PMESII allows for the proper prioritization and allocation of resources to accomplish assigned tasks and gain leverage, as needed. Strategic guidance delivered from higher authorities establishes context for analyzing the operational environment and provides JFCs the ability to organize forces to meet the conditions presented. As stated, alignment and responsibilities of forces, whether service- or joint-led, traditionally fall within a domain-centric construct. Thus, JFCs will determine the appropriate structure for their organization to plan for and execute domain control operations, commensurate with the operational environment and the strategy that guides them.

---

[24] JP 3-0, IV-1.
[25] JP 3-0, IV-1.

As implied in Joint Publication 3-0, military strategy tends to emphasize the control of physical domains (including space) through the exploitation of the information environment, or cyberspace. Information forms the hub of military activities and ultimately exists to support decision-making at all levels of war. A final review of conventional methods of military strategy and planning broadly explores how joint planners incorporate information requirements into campaign plans and how JFCs currently conceive and organize for information superiority.

JFC Decision-Making, Information Operations, and . . . Cyberspace

The first two chapters discussed the evolution of information technologies over the past two centuries and their influence on war's character. Information—historically considered a prized commodity—was always in high demand, and commanders structured their forces in ways that compensated for a perennial lack of communication capabilities. As examined, Moltke formed the general staff to direct more complex arrangements of forces along an expansive battlefield. Moltke's solution alleviated a growing challenge for commanders and essentially redefined the military command structure. Today, staffs continue to assist commanders with assessing operational environments, identifying problem sets, deriving options, and distributing orders. Theoretically, the core function of the command staff fulfills the critical requirement of decision-making in times of crisis. Dr. Jeffrey Reilly, a proponent of operational design, writes, "Operational environments are constantly in a state of change, and when staffs assist commanders in understanding decision criteria and risk mitigation the commanders are much more likely to act decisively."[26]

Current joint doctrine reveals a growing appreciation for the complexities involved with information superiority and decision-making in war. Joint Publication 3-13, *Information Operations*, captures the foundational precepts of decision-making and decision paralysis highlighted by Sun Tzu, Liddell Hart, J.F.C. Fuller, John Boyd, et al. The Secretary of Defense defines information operations "as the integrated employment, during military operations, of IRCs [information-related capabilities] in concert with

[26] Jeffrey M. Reilly, *Operational Design: Distilling Clarity from Complexity for Decisive Action*, (Maxwell Air Force Base, AL: Air University Press, 2012), 1.

other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own."[27] Furthermore, joint doctrine views information operations (IO) as a means for achieving information superiority, defined as "the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[28] Several joint documents further describe how JFCs can organize and task their units to conduct IO and achieve information superiority in an increasingly multifarious environment.

Reviewing broad concepts of IO and associated force structures provides a basis for understanding current operational paradigms regarding information, decision-making, and strategy. First, IO involves protecting information-related capabilities to secure friendly decision-making opportunities and therefore encompasses a larger range of considerations than the theoretical model proposed in Chapter 2.[29] As discussed, joint planning staffs absorb JFC strategic intent into campaign-plan development and analyze the operational environment to extract relevant problem sets and derive possible courses of action (COA). At each stage of development, JFCs and their staffs may form decision criteria that provide flexibility and relative stability to the operation. Once a COA is selected, planners refine COA-specific decision opportunities based on the approved strategic concept. Most importantly, each decision point is enabled through the collection and dissemination of decision-specific information in the form of commander's critical information requirements, or CCIRs. Critical information requirements include details on friendly and enemy activities, termed friendly force information requirements (FFIR) and prioritized intelligence requirements (PIR), respectively. Decision points and their associated CCIRs comprise the supporting elements of a commander's decision-making process during campaign execution and provide needed focus for information collection and dissemination efforts.[30]

---

[27] JP 3-13, ix.
[28] JP 3-13, GL-3.
[29] Recall that Chapter 2 emphasized the preservation of organic essentials, or the information pathways comprised of physical networks upon which messages are transmitted and received. Current IO doctrine ultimately focuses on manipulating decision making through control of the strategic message itself, an endeavor that exceeds the intent of this analysis.
[30] For additional details on joint operational planning, reference Reilly, 73-77, 80.

Anticipating all possible decision points is impossible, but JFCs and their staffs can build preplanned decisions into a COA based on analysis of the operational environment and strategic intent. These decisions may include reapportionment of forces, prioritization of component efforts, or approval for contingency operations (i.e., branch plans). Joint planning staffs may capture these overarching decision points in a decision support matrix (DSM), a quick-reference tool for commanders to employ during execution. Of note, DSMs typically include respective CCIRs and decision criteria based on the overarching strategic concept (see Figure 6). Joint planning staffs may also anticipate dynamic or ad-hoc decision-making opportunities, but the ability to identify such events during execution is dependent upon the sustained flow of relevant information throughout the course of the operation.[31]

Sample Decision Support Matrix (For JFC)			
Decision Point	**Decision Required**	**CCIRs**	
		PIR	**FFIR**
#1	Commit operational reserve to stop penetration of Forward Edge of the Battle Area (FEBA)-A along coastal avenue of approach (AA) **ISSUE WARNING ORDER:** 1) Authorize JFLCC to issue warning order to operational reserve (MEB) to block penetration of FEBA-A along coastal AA 2) CHOP MEB to JFLCC	1) Enemy forces threaten brigade size penetration of FEBA-A 2) Enemy forces preparing to move "XY" Armor Brigade in vicinity of "Z"	Friendly forces at less than 80% strength
	ISSUE EXECUTIVE ORDER: 1) Deploy MEB ashore 2) Authorize JFLCC to commit MEB to block penetration of FEBA-A along coastal AA	Enemy brigade at greater than 70% strength has penetrated FEBA-A	1) Air and fires are insufficient alone to stop penetration 2) Friendly forces less than 70% strength 3) Friendly reserve already committed

Figure 6: Sample JFC DSM
Source: Adapted from Jeffrey M. Reilly, Operational Design: Distilling Clarity from Complexity for Decisive Action, (Maxwell Air Force Base, AL: Air University Press, 2012), 77.

From an information protection standpoint, information assurance (IA) actions are designed to secure information systems and the information they collect and

[31] The capacity to make ad-hoc decisions and act in a timely and appropriate manner is best illustrated through John Boyd's OODA loop model, discussed in Chapter 1.

disseminate.[32] At present, military information systems are consolidated in the Department of Defense Information Network (DODIN). The DODIN incorporates a "globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policymakers, and support personnel."[33] Furthermore, in fulfillment of information assurance, and in support of IO, DODIN operations "are actions taken to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation."[34] At the campaign level, joint forces rely on DODIN and information assurance activities to support decision-making requirements outlined in operational plans.

The second and more accentuated aspect of IO involves information denial or disruption to affect adversary decision-making. Chapter 1 detailed Boyd's concepts of strategic paralysis and Liddell Hart's depiction of displacing an adversary's psychological and physical balance. In Boyd's OODA loop, emphasis rests with the second step, *Orient*, or how a decision-maker (man or machine) interprets information collected through observation and assesses its relevance for action. Information operations therefore target an enemy's ability to orient to his observed environment by either saturating him with too much data or intentionally manipulating the data to the point where he no longer has confidence in its reliability, thereby preventing accurate and timely decisions for action. Ultimately, information operations, through information assurance and information disruption, support the propagation of strategic narratives aimed at influencing target audiences and reducing their ability or desire to resist. Acceptance of this approach generates the impetus for information operations and information superiority, and joint operations seek to exploit current advantages in information technologies to achieve such effects.

The third and final aspect of IO encompasses the organizational structures and tasks associated with current IO practices. How a JFC arranges forces and conducts

---

[32] JP 3-12(R), GL-4.
[33] JP 3-12(R), GL-4.
[34] JP 3-12(R), vii.

information operations for information superiority is a key indicator of conventional paradigms. In essence, theater IO focuses primarily on the management of information itself and the coordination of a consistent narrative (i.e., identification of target audiences, how and when to transmit information, information protection, and how information is received and/or interpreted). Joint doctrine incorporates capabilities from a wide range of disciplines in its IO mission set, including strategic communications, public affairs, cyberspace operations, space operations, military information support operations (MISO), intelligence, military deception, and operations security (OPSEC).[35] To this end, the CJCS maintains the Joint Information Operations Warfare Center (JIOWC) to help coordinate the integration of various information-related capabilities within a specific combatant command (CCMD). At the CCMD level, JFCs are given leeway on how to manage IO efforts in theater. Theater commanders may form an IO staff at the JFC (or CCMD) level to provide "command-level oversight and collaborate with all staff directorates and supporting organizations," including the JIOWC.[36] Joint force commanders may further create an IO cell to support the generalized IO staff that specializes in these disparate and complex IO functions. The proper orchestration of information protection and messaging is considered a way to control the information environment, and the JIOWC, IO staff, and IO cell provide JFC oversight accordingly.

From an information systems perspective, communication networks comprise the physical elements of the information environment and are seen as the supporting architecture for IO. Generally, a JFC employs a joint communications directorate, designated the J-6, to manage information system requirements and ensure CCMD connectivity.[37] The J-6 coordinates with theater components to determine informational needs and collaborates externally with USSTRATCOM for the establishment and management of the DODIN, discussed previously. In turn, CDR USSTRATCOM typically delegates responsibility for military cyberspace operations to United States Cyber Command (USCYBERCOM), a sub-unified command activated in 2010. Today,

[35] The Commander, United States Special Operations Command (USSOCOM) is responsible for integrating and coordinating MISO in theater while the Commander, United States Strategic Command (USSTRATCOM) coordinates electronic warfare and cyberspace operations in support of JFC IO objectives. Reference JP 3-13, xii.
[36] JP 3-13, x-xi.
[37] For additional details on standard J-6 responsibilities, see Joint Publication 6-0, *Joint Communications System*, 10 June 2010, xiii-xvi.

USCYBERCOM assigns Cyber Mission Teams (CMT) to theater JFCs, as required, to accomplish its missions in theater.[38] The CMTs integrate defensive and offensive cyberspace operations in fulfillment of information assurance and denial requirements, respectively, as outlined through the JFC's IO requirements.

The creation of USCYBERCOM and its expanding role reveals a gradual consolidation and alignment of information operations under cyberspace. In other words, corresponding to domain-oriented structures detailed earlier, *joint doctrine aligns information security and information disruption primarily with the cyberspace domain*. Most tellingly, JP 3-0 considers the information environment (i.e., cyberspace) "pervasive to all activities worldwide and to the air, land, maritime, and space domains of the JFC's operational environment," indicating a distinction in the functional relationship between cyberspace and its counterparts in joint operations (the implications of which undergo scrutiny in the next section).[39] Furthermore, protection of the DODIN and the information environment writ large, key aspects of a JFC's information assurance mission, are supported by USCYBERCOM through its CMTs (along with the J-6 and IO staff, if created). Fittingly, "Cyberspace capabilities requiring protection include not only the infrastructure (computers, cables, antennas, and switching and routing equipment), as well as parts of the EMS (e.g., datalink frequencies to include satellite downlink, cellular, and wireless), and the content (both data and applications) on which military operations rely."[40] Thus, cyberspace, the primary component of the information environment, now embodies the IO domain designation for the joint force.

Two final and critical points emerge from this current approach to IO, both of which demand close analysis as the United States strives to acquire domain control in the Information Age. The first point involves the conceptual distinction of cyberspace from the *physical* domains of land, air, maritime, and space and the direct relationship between

[38] From USCYBERCOM Mission statement: "USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks [DODIN] and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries." United States Strategic Command. "United States Cyber Command Fact Sheet," http://www.stratcom.mil/factsheets/2/Cyber_Command (accessed 23 March 2015).

[39] JP 3-0, IV-2.

[40] JP 3-12(R), viii.

cyberspace operations, IO, and information superiority. Specifically, while incorporating cyberspace as the principle information domain, joint and service doctrine delineate space from the information environment (and therefore cyberspace) by describing it as a physical domain within the JFC's operational environment. The second point references the organizational approach to IO (cyberspace), discussed above. Of significance—because cyberspace is considered a global domain—a JFC's IO staff, IO cell, J-6 directorate, and CMT activities are not consolidated under a distinct theater component command, commensurate with the components for air, land, maritime, or even special operations. Although USCYBERCOM is developing a joint functional cyber component command (JFCCC) construct for theater JFC support, USSTRATCOM's space component, the Joint Functional Component Command for Space (JFCC SPACE), does not have an equivalent initiative, nor is it integrated within the JFCCC model. The implications for these conceptual and organizational approaches to IO (and, by extension, information superiority) are worth investigating, and the theoretical framework outlined in Chapters 1 and 2 provides requisite context for evaluating current warfighting doctrine.[41]

A New Paradigm for Information Age Warfare

A return to the discussion on grand strategy offers insight into the unchanging role of military operations and its manifestation in the Information Age. Grand strategy articulates national interests and is influenced by cultural values and perceptions. Among national values is the expectation (acceptance and willingness) of the use of force to promote or secure national interests. Since the end of the Cold War, public and political expectations of military force were shaped by the capabilities afforded by information technologies. Additionally, the same information and communication networks redefined qualities of life in industrial societies, empowering and subsuming all national and military activities (the United States reaped its benefits in a unipolar setting). As stated, grand strategy and its subordinate strategies codify (explicitly and implicitly) national

[41] Current joint doctrine places minimal emphasis on space control as a function of IO. JP 3-13 (Information Operations) does not list a space element in its notional IO cell but includes a cyberspace position. Furthermore, JP 3-14 (Space Operations) only mentions "information superiority" once. For further information, reference JP 3-13, xi-xiii.; and JP 3-14, I-4.

values that are worth preserving. In twenty-first century warfare, these values are expressed through the application of highly lethal, versatile, and precision firepower with limited-to-no collateral damage and equally minimal risk to US and Allied personnel.

As indicated in the preceding chapters, modern expectancies of non-linearity, flexibility, efficiency, adaptability, et al. emerge from the existence of global communication networks that enable mass connectivity, communication, and collaboration. Figure 7, first revealed in Chapter 2 (see Figures 2 and 4), demarcates the region where the US military intends to operate in future conflicts from a firepower and force size perspective (particularly in an age of reduced budgets)—both of which are determined by the availability of near instantaneous and networked information. Enticing concepts of full-spectrum superiority and cross-domain operations, highlighted earlier, reside in the shaded region depicted in the chart, and information networks serve as the connective tissue that binds activities across multiple domains. *In essence, the shaded region denotes the US military's underlying strategy for conducting war*.[42] If the United States aims to preserve its desired way of life and way of warfare, it must place great emphasis on securing the capabilities that facilitate them. To this end, *the United States should adopt a comprehensive information control strategy that seeks to identify and secure access to the space and cyberspace systems that increasingly facilitate its way of life and desired way of warfare*.

As Figure 7 illustrates, at least two inflection points exist (yellow dots), the first being the arbitrary region that bounds the desired way of warfare and the second, more significant pivot exists at the notional regression point from Information Age warfare back to Industrial Age warfare (i.e., mass concentration of force and mass destruction). Therefore, Information Age warfare exists first to ensure that military operations sustain the desired balance between precision firepower and force size, made possible through the exploitation of full-spectrum superiority and cross-domain operations. In this context, the analysis now turns to transposing proposed theoretical concepts of information warfare (i.e., information control and superiority) on the conventional approaches dissected above.

---

[42] In this sense, the US military's desired way of warfare is described as the ability to concentrate lean, disparate, and geographically dispersed units at a specific time and space for precision engagement.

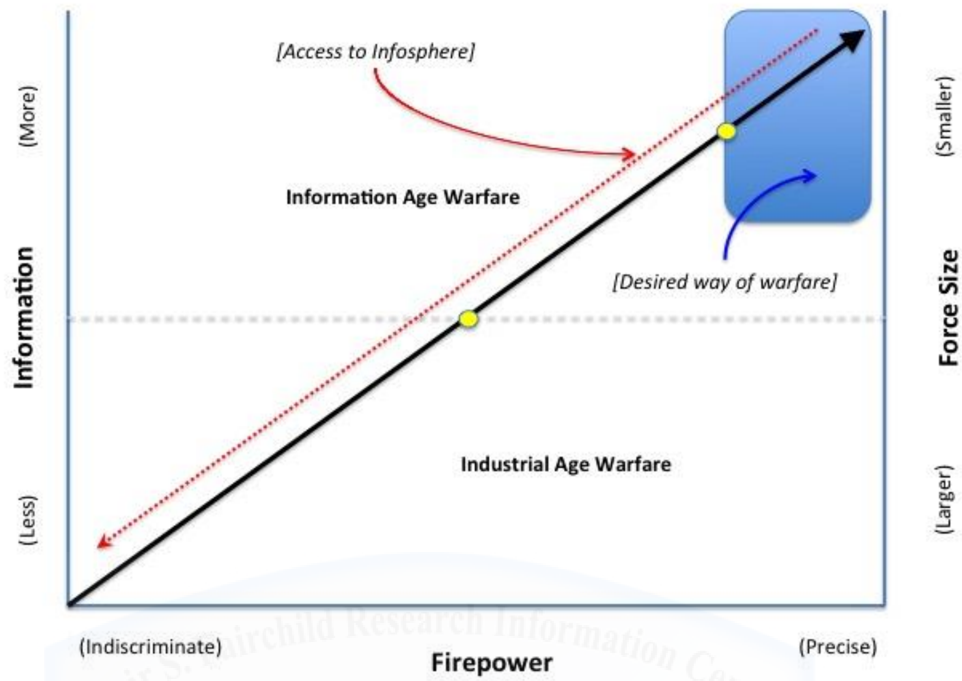

Figure 7: US Military's Desired Way of Warfare (Notional) in the Twenty-First Century
Source: Author's Original Work

Modified Definitions of Information Control and Information Superiority

Under this new paradigm, information control is now a foundational, strategic requirement along the spectrum of peace and war. Relatedly, Chapter 2 expressed the global infosphere as a principle phenomenon of the Information Age. Therefore, an operational model for Information Age warfare begins with the *deliberate identification and control of infospheres* that support strategy development, execution, and assessment. Again, the term *infosphere* is used in lieu of "information environment" due to its descriptiveness of the surrounding nature of global information networks—particularly the physical and information (virtual) dimensions surrounding specific strategies. As described in Chapter 2, infospheres are scalable and malleable: infospheres concurrently exist at the strategic or global level (enabling broad, enduring national endeavors) and theater level (encompassing campaigns, operations, missions, and unit activities) and are configured based on fluctuating informational needs. Informational needs in twenty-first

century warfare are dictated by strategy, resultant decision-points, and the weapon and C4ISR systems employed to project and employ force.

Combining theoretical concepts from the first two chapters provides a new framework for information control and information superiority in the modern era. Strategy and decision-making drive information requirements that set the foundation for an infosphere. As stated, infospheres include physical, information, and cognitive dimensions; each interrelated to deliver support for decision-making and action. Decision-making opportunities, involving man and machine, reside in the infosphere's cognitive dimension, while information (and raw data) naturally comprises the information dimension. The physical dimension includes the information technologies (i.e., platforms, systems, and networks) that collect and disseminate requisite information as determined by strategy. From Chapter 1, information collection technologies are identified by their access and methods (or sensors) while dissemination capabilities are characterized by reach and speed.

In this sense, the physical dimension constitutes the focus of infosphere control. Information requirements begin with (and support) strategy development and flow from the cognitive dimension, which interprets data and makes decisions to act. As codified in joint IO doctrine, the information itself is the most critical component—indeed, it is considered "ground zero" in the pursuit of information superiority.[43] Nevertheless, the physical dimension forms the cornerstone of any infosphere and yet is often overlooked from an integration, protection, and exploitation standpoint. The cognitive dimension will atrophy and the information dimension will lose its relevance without proper collection and dissemination capabilities in place. Similarly, the information technologies and networks that comprise the infosphere are only as applicable to a particular strategy as the information they collect and disseminate. Hence, controlling or ensuring access to the information systems contained within one's infosphere (and selectively denying the adversary access to his own information systems, as required) serves as a precursor for gaining information control and, subsequently, information

[43] David S. Alberts, John J. Garstka, Richard E. Hayes, and David A. Signori, *Understanding Information Age Warfare*, (Washington, DC: DoD Command and Control Research Program, 2001), 13.

superiority. From this construct, *information control and information superiority start with an infosphere's physical dimension*.

Building on the conventional concepts of domain control and domain superiority presented earlier, a revised description of information control follows: Control is about dictating actions (or the ability to dictate actions) in a certain region. *To this end, information control involves freedom of access, maneuverability, and exploitation of established infospheres*—commensurate with one's strategy—*and the ability to prevent others from removing that freedom. Control of the infosphere begins with controlling access to the physical dimension, or the information collection and dissemination systems employed*. Furthermore, *information control emphasizes defensive capabilities for its attainment*. In this sense, control is distinct from superiority in that it provides assured access to an infosphere but does not involve a comparative advantage.

Information superiority, on the other hand, implies a relational construct that measures the degree of infosphere control one side has compared to another's *based on the respective needs of their competing strategies*. Thus, *information superiority involves a relative condition of control—one side is able to control infosphere access as needed, while the opponent is not able to exert the level of control required by his strategy*.[44] For example, if one side relies less on space capabilities but is still able to exploit the domain to meet the informational demands of its strategy, then the opposing force cannot claim information superiority based on that fact alone. The first force can simply claim information control if the opponent is unable to prevent freedom of access to his infospheres. If the same force maintains the requisite amount of information control and can *also* eliminate the opponent's ability to access, maneuver, or exploit his infospheres, *as he needs*, then the first force can claim information superiority.[45] In this light, whereas defensive capabilities are best suited for information control, *offensive capabilities are*

---

[44] Recall the current definition of information superiority: "The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." While possibly implied, the definition does not clarify the relationship between the information *required* and the associated information systems employed to collect and disseminate. Reference JP 3-13, GL-3.

[45] A space power at war against a non-space power, for example, will inherently produce greater options for gaining an information advantage, but having increased options or capabilities does not automatically translate to information superiority. The ability to exploit relevant, timely, and accurate information based on strategic, operational, and tactical needs while preventing the enemy's ability to do the same constitutes the premise of information superiority.

optimized for gaining information superiority. From an Information Age warfare standpoint, these revisions of control and superiority apply to the comparative control of infospheres employed by each side during their duel.

Revising the Domain Construct for Space and Cyberspace

At this point, another key revision of traditional concepts emerges. In its current depiction, an infosphere's physical dimension involves collection and dissemination technologies and, by extension, the domains within which they operate. Previously mentioned, of the five traditional joint operating domains, space and cyberspace represent the two employed primarily (or explicitly) for information purposes. Indeed, at their core, *common space capabilities are inherently informational capabilities*.[46] Furthermore, space architectures—discussed in the last two chapters—are connected via global space and cyberspace networks, while cyberspace operations employ space capabilities to enhance (or even empower) their utility.[47] In effect, space and cyberspace already operate within an integrated web of information collection and dissemination processes.[48] As such, space and cyberspace assets are only as valuable as 1) their location (accessibility) relative to the information required, 2) their ability to maneuver or reach a position capable of acquiring or disseminating requisite information, 3) the technology available to acquire information once physically (or virtually) in place, and 4) the security and robustness of the communications networks established to distribute the information to users. Therefore, in reality, space and cyberspace are actually complementary components of a larger construct—that of information control and information superiority (through initial control of the infosphere's physical dimension).

By design, then, infospheres expand on conventional depictions of the information environment to incorporate cyberspace and space technologies as the

[46] Common space capabilities include but are not limited to: overhead imagery (e.g., electro-optical and multi-spectral); weather forecasting; infra-red (IR) detection for missile warning and terrestrial defense systems; global and regional satellite communications (SATCOM); data relay (e.g., Internet and cell phone communications); space surveillance; and position, navigation, and timing (PNT).
[47] Reference P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, (New York, NY: Oxford University Press, 2014), 14.; and JP 3-12(R), I-2.
[48] JP 3-12(R), I-2. "The relationship between space and cyberspace is unique in that virtually all space operations depend on cyberspace, and a critical portion of cyberspace can only be provide via space operations. Space provides a key global connectivity option for [cyberspace operations]. Conversely, [cyberspace operations] provide a means by which space support is executed."

consistent backbone of the physical dimension. Contrary to current joint doctrine, from an information perspective, space and cyberspace capabilities are compared in terms of their *functional* rather than physical or virtual qualities of their respective domains.[49] Instead of categorizing space as one of four physical domains within a JFC's operational environment, space and cyberspace—while distinct—are conjoined as foundational domains of an infosphere. Indeed, functionally, space and cyberspace now appear more closely related than space and air, and certainly more intertwined than space, land, and sea domains. This new construct may alter the way in which JFCs allocate domain roles and responsibilities, particularly from an air component (COMAFFOR) standpoint.

Implications for the Joint Force

The imperative behind such a change rests in the basic premise of Information Age warfare and the factors illustrated in Figure 7. An entirely new, or substantially revised, strategy emerges in the twenty-first century, corresponding with the rapid growth of the infosphere, the primary artifact of the age and a new strategic front. Assuming the United States intends to preserve its current way of life and desired way warfare, strategy—at all levels—must now include provisions to deliberately and comprehensively define and secure the infospheres it employs. Modern concepts of national prosperity, national security, force projection, and force employment are built on the assumption that information networks are and will be available. Thus, a failure to adequately identify and secure infospheres that support strategy development and implementation may degrade or even prevent the United States from achieving its objectives in future conflicts. *An enduring and prioritized pursuit of information control (and information superiority) via control of infospheres now drives the new strategic approach to warfare*.

By comparison, the emphasis on information control by securing access to infospheres holds similarities with recent concepts of air power. Warden's belief that air superiority preceded all other activities on land and sea formed his strategy of using air power to isolate enemy C2 capabilities and critical civil and defense infrastructures. In

[49] While interrelated functionally, concepts of operation in space and cyberspace (e.g., concepts of maneuver, fires, and logistics) are different and therefore still warrant their domain distinctions.

essence, Warden viewed air power as the leading edge in an offensive front, paving the way for terrestrial forces to maneuver and advance. Information control, at a minimum, functions in the same capacity, although it encompasses all operations independently and congruently. In this regard, national sources of power, force projection, and force employment inherently subsist within the confines of strategic and theater infospheres. Therefore, the establishment and protection of infospheres are prerequisites for any action taken on behalf of national interests.

This new approach generates a forcing function for the integration of space and cyberspace doctrines, strategies, and operations under an overarching information control strategy. By consolidating space and cyberspace as the primary information domains (perhaps the most significant assumption for domain operations), identification and protection of infospheres now includes the coordinated identification and protection of space and cyberspace systems that comprise them. Identification and prioritization of systems initiates with the information requirements established by strategy and the cognitive elements (man and machine) situated for decision-making and action. Protection and control of space and cyberspace systems involves integrated offensive and defensive space and cyberspace operations—designed to deny an adversary's access to his own infospheres while protecting one's own, thereby achieving information control and superiority. In sum, all space and cyberspace operations now flow from a common imperative.

Most significantly, this adjusted approach to Information Age warfare drives a profound change in the utility and resultant value of gaining and maintaining space and cyberspace control. Contrary to conventional perceptions, domain control in space and cyberspace is now driven by the requirement to identify and secure access to the physical dimension of the infosphere. Put differently, controlled access to an infosphere is only possible through controlling access to the integrated space and cyberspace networks that comprise it. Thus, using the modified definitions of control and superiority above, *space and cyberspace control are subsets of information control, and, by extension, space and cyberspace superiority are the two elements necessary for achieving information*

superiority (see Figure 8).[50] The implications for joint and service components are considerable, and Chapters 4 and 5 examine the significance (and feasibility) of this new methodology on current space operations.

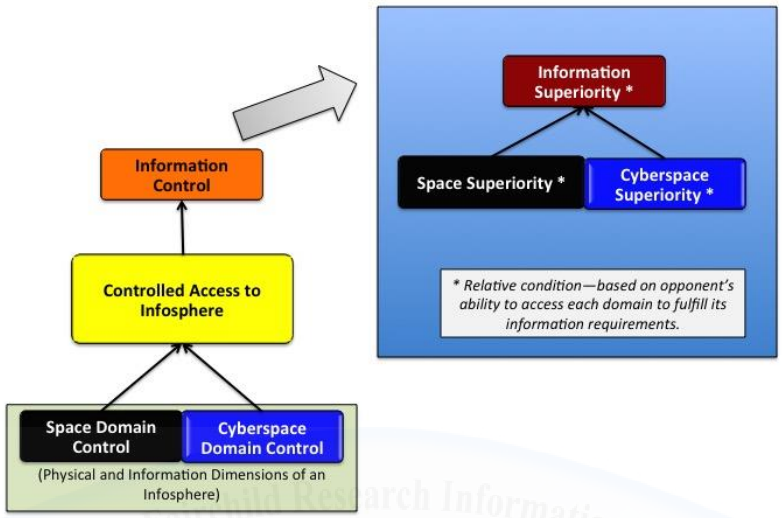

Figure 8: Relationship Between Space, Cyberspace, and Information Control / Superiority
Source: Author's Original Work

Operational Examples

Although not all-inclusive, a few operational and tactical examples are provided to illustrate how the new strategic approach manifests itself in warfare, particularly from the perspectives of strategy development, decision-making, force projection, and force employment. Of note, these examples are simplified and are only intended to highlight general differences in operational methods or priorities. First, as part of strategy development, joint intelligence preparation of the operational environment (JIPOE) activities initiate with the information and intelligence requirements levied by decision-makers in a particular region. In this endeavor, space and cyberspace collection and dissemination networks are collectively established at various levels (global, theater,

[50] The feasibility of cyberspace control or superiority is not universally accepted. However, as Singer and Friedman suggest, cyberspace—while primarily virtual in nature—upholds traditional concepts of domains by virtue of its physical elements. "[Cyberspace] relies on physical infrastructure and human users who are tied to geography, and thus is also subject to our human notions like sovereignty, nationality, and property." See Singer and Friedman, 14.

regional, etc.), providing the backbone for augmented ISR systems within the physical domains of air, land, and/or sea. Importantly, JIPOE for an information control strategy also helps anticipate enemy information requirements to model the enemy's possible infospheres—known or unknown—that contribute to his strategy, *supporting friendly offensive space and cyberspace options in the pursuit of information superiority*. Friendly space and cyberspace networks, alongside to other ISR systems, form the physical dimensions of the infospheres supporting JIPOE and are prioritized and defended based on specific intelligence requirements.

In support of decision-making, a return to the decision support matrix (DSM) detailed earlier is warranted. As shown, DSMs relate a commander's critical information requirements (CCIRs) to their respective decision point(s) and aid the commander by consolidated triggers for initiating a decision. However, the DSM does not include systems and or sources available (or assigned) to collect and disseminate the CCIRs needed for each decision point. Furthermore, no document or planning process directly connects the information systems to the decision points they support. At best, the information networks involved in collecting and distributing CCIRs remain buried within component and unit level plans, or are handled by a conglomerate of IO staffs, J-6 directorates, the JIOWC, USCYBERCOM, the intelligence community, et al. In essence, conventional processes isolate information systems from the decision points they support at the operational and tactical levels, preventing decision-makers (and planners) from having situational awareness on their ability (or inability) to provide data in a timely manner. This critical discrepancy may negate any decision advantage gained through utilizing the DSM. In the new paradigm, however, the DSM drives the creation of one or more infospheres by first establishing information networks across space and cyberspace and then "plugging" any other collection and dissemination technologies from air, land, and sea into the combined space and cyberspace complex. These networks, prioritized by their relationship to key decision points, subsequently dictate combined defensive space control and defensive cyberspace operations, as applicable, designed to ensure availability of CCIRs for decision-making and action in non-permissive environments.[51]

[51] In the new paradigm, conventional requirements for defensive space control (DSC) and defensive cyberspace operations (DCO) may also change, although the specifics lie beyond the scope of this analysis.

Information control as a general strategy also revises operational concepts of force projection and force employment. In the twenty-first century, all sources of national power—and particularly military force—are projected in and through an intricate web of enabling infospheres. Militarily, the global dispersal of maritime forces, air mobility operations, and global strike missions collaborate and maneuver within a series of associated infospheres (theater and strategic) that enable their functionality. Furthermore, C2 is made possible through imbedded information technologies that connect decision-makers with the forces they lead around the globe. In each case, unique mission needs (e.g., decision-points, weapon system communication capabilities and requirements, etc.) dictate the characteristics of the infospheres that support them. Regardless of a mission's nature, all communications will inevitably reconnect into a larger information network bounded by space and cyberspace systems. Therefore, as strategists and planners organize force projection and employment campaigns, operations, and missions, they now incorporate information control models into their calculus.

Creating and managing a strategic information landscape for force projection and employment ensures greater fidelity for planners to identify and protect specific space and cyberspace systems that enable each mission (strategic, theater, and tactical levels). For instance, as air mobility assets and carrier strike groups traverse the globe and transition between multiple geographic combatant commands, associated information control plans include the physical (and integrated) space and cyberspace systems employed for the tasked mobility and naval fleet forces as well as their distant C2. Likewise, strike packages involving net-centric air superiority fighters (e.g., the F-22 Raptor and eventually the F-35 Lightning II), CONUS-based global strike assets (e.g., the B-2 Spirit), and supporting ISR assets such as remotely piloted vehicles (RPV) will include specific space and cyberspace systems that enable weapon system functionality as mission critical assets in the operation, in turn setting space and cyberspace control priorities. Finally, non-lethal and non-kinetic strike operations (e.g., electronic warfare) in and through space and cyberspace are enabled through information control

operations—offensive space and cyberspace tasks rely on access to their respective infospheres just as their counterparts in air, land, and sea.[52]

A deliberate and integrated information control plan—fusing space and cyberspace operations under one strategic model—provides an opportunity to coordinate such complex endeavors. Information control through the creation and protection of infospheres based on strategic and tactical requirements ensures access to required information in non-permissive environments. At present, military planners function with an amalgam of complicated, heterogeneous communications networks with bureaucratic anomaly resolution processes performed by external agencies not always associated with or aware that operations are underway. Furthermore, joint warfighters—in all domains—are typically not aware of the systems providing critical information, preventing adequate assessments on the significance of system degradations to mission accomplishment (or decision-making)—in this case, everything or nothing becomes a priority for protection. The new approach offers strategists, planners, and tacticians direct insight into which information capabilities are employed to enhance or enable operations. As a result, the degradation of physical networks within an infosphere due to the loss of collection and/or dissemination capabilities may now trace directly back to mission-specific and strategic consequences. Ultimately, the strategic concept of information control is designed to preserve the desired way of warfare, a significant undertaking.

Challenges Associated with the New Paradigm

The new approach to Information Age warfare addresses several key issues facing an Industrial Age force transitioning to the realities of emerging strategic environments. First, it offers a new paradigm for approaching information control in a complex, globalized network by re-categorizing space and cyberspace operations as equal components of information operations (with greater implications for space than cyberspace). Second, establishing this information control methodology as a strategic priority for force projection and employment creates an imperative to coordinate information control strategies with joint planning and execution processes. Deliberately

---

[52] From this perspective, control of the infosphere is a *precursor* to exploiting joint information operations (IO) outlined in the previous sections.

integrating information control strategies with each theater strategy, campaign, operation, and mission exponentially enhances shared awareness for true cross-domain operations and full spectrum superiority—when a satellite or cyber system is lost, *all* participants recognize the implications and can adapt accordingly.

The approach also highlights new challenges, however, four of which are highlighted here. One potential challenge, more operationally focused, involves determining when sufficient information control is attained, both spatially and temporally. As stated, information control initiates with the identification and protection of the physical dimension, but the ultimate goal is to secure access to relevant information based on one's strategy. One potential approach to assessing information control in the information dimension is offered by Singer and Friedman. They offer three goals for cyberspace security that notionally extend to information security (or information assurance, IA) writ large: information confidentiality, integrity, and availability, otherwise known as the "CIA triad." Confidentiality seeks to maintain information privacy and employs software mechanisms such as encryption. Integrity is the most complicated yet substantial goal as it relates to the purity of data and the information systems that collect and distribute it. Availability refers to the proper functionality of an information system's hardware and software.[53] All three goals involve several layers of operational considerations and demand rigorous analysis. As a general concept, provisions must be in place to verify that an infosphere's physical and information dimensions maintain information assurance, and the "CIA triad" may offer a useful point of departure for establishing verification criteria. Such an assessment is necessary for confirming the attainment of information control and even establishes broad metrics for space and cyberspace control.

Second, complete identification and protection of an infosphere is extremely difficult, if not impossible. From an attack perspective, the sheer complexity of an infosphere's physical network is such that any attempt to prevent access could only realistically generate system degradation rather than complete denial. Additionally, dispersal or disaggregation of information systems may further complicate an enemy's ability to affect an infosphere's physical and information dimensions. However, the

---

[53] Singer and Friedman, 35.

probability of infosphere degradation over complete denial creates an impetus for thoroughly understanding how infospheres (and specifically their physical systems) are integrated into operations. As shown in Figure 7, several inflection points exist where reduced availability of requisite information will limit or even prevent the accomplishment of activities and outcomes. The challenge thus rests with the ability to recognize or foresee when the inflection points occur over the course of an operation, demanding close assimilation of information requirements and associated information systems into operational plans. When prioritized space and/or cyberspace systems are attacked, strategists and warfighters (across the entire joint force) must understand the implications to their specific operations and ensure contingency options remain available. The identification and protection of physical information systems—and an understanding of operational impacts due to their degradation—invokes a significantly greater level of coordination between space, cyberspace, and other domains than currently afforded.

A third, more encompassing challenge stemming from this new way of warfare is the likely emergence of unforeseen regions of strategic value in future wars. Formally establishing the infosphere as a strategic environment issues new difficulties in recognizing or anticipating strategic chokepoints and vulnerabilities. A brief review of the Pacific Theater in World War II provides unique perspectives on how new methods of warfare create unique areas of strategic importance. At the time, air power as an instrument of war was still in its infancy. Consequently, Japanese and American strategists initially failed to appreciate the strategic importance of the South Pacific in achieving their objectives. As conflict ensued, the South Pacific soon arose as a vital region in the war with both sides battling to gain control of the territory and generate leverage. In essence, the very nature and importance of air power made the South Pacific invaluable to each side's strategy. As historian Eric Bergerud noted, "there was nothing of inherent importance to attack or defend" in the South Pacific, therefore "the airbases themselves became the only strategic objects of importance."[54] Eventually, what was once seen as an optimal staging area for projecting power turned into the *primary* theater of operations, requiring tremendous amounts of national resources and the meticulous

[54] Eric Bergerud, *Fire in the Sky: The Air War in the South Pacific*, (New York, NY: Basic Books, 2009), 6-7.

coordination of land, air, and sea capabilities.[55] Fortunately, due to superior technologies, industrial capacities, training, and manpower, the United States was able to recognize, adjust to, and exploit the strategic landscape better and faster than the Japanese.

A fourth significant consideration yet unmentioned involves the reallocation of resources, authorities, roles, and responsibilities for generating and implementing information control strategies. As it stands, the scope and depth of information control demands resources and authorities that exceed current levels allocated by joint doctrine. *The proposed method for gaining information control inherently warrants its own global strategy with subordinate campaign efforts—distinct from yet synchronized with theater campaigns.* Moreover, *geographic combatant commands are not postured or designed to develop and implement such information control campaigns in addition to their UCP-directed charters*.[56] By the very nature of globalized information networks, a single command structure is necessary for establishing information control strategies and priorities and orchestrating space and cyberspace functions in concurrent support of national and theater activities. United States Strategic Command currently houses USCYBERCOM and JFCC SPACE, but the two sub-entities are not functionally bound, as previously indicated, and therefore develop their strategies, priorities, command structures, and requirements under current parochial paradigms. At a minimum, USCYBERCOM and JFCC SPACE should exist as equal components of a unified combatant command designed for orchestrating information operations at all levels of war. If USSTRATCOM assumes this responsibility, the Defense Department should consider realigning USCYBERCOM and JFCC SPACE under an information control construct within the existing combatant command.

The sheer complexity of information control strategies suggests a dangerous set of circumstances could develop in the next battle for information control and information

[55] Bergerud, 659.

[56] Interestingly, Colonel John Warden received harsh criticism for using the term "air campaign" during the creation of Instant Thunder, the spiritual predecessor to the air effort in Operation Desert Storm. "Critics objected to Warden's use of the term 'air campaign': in their view there could be only one 'campaign'—the joint military campaign—and everything else was an operation supporting that campaign. Others strongly believed that air forces were so fully integrated into the warfighting force as a whole that the concept of an independent air campaign made no sense." See John Andreas Olsen, *John Warden and the Renaissance of American Air Power*, (Washington, DC: Potomac Books, Inc., 2007), 78.

superiority. In future wars, joint forces may find themselves deeply engaged in regions in space and/or cyberspace (or even terrestrially) that they did not anticipate. Moreover, JFCs may not have the infrastructure in place to verify information assurance in degraded environments. Accepting the theoretical construct for information control now may minimize such experiences as national and military organizations continue acclimating to Information Age warfare. Most importantly, for the military to adequately transform its operations, acceptance of the Information Age warfare model must occur across the *entire* Department of Defense and may drive a realignment of authorities, roles, and responsibilities at the combatant command level.

Summary and Synthesis of the New Information Control Paradigm

The new archetype presents several new considerations for conceptualizing Information Age warfare, some more theoretical than others. Nonetheless, the ideas presented serve as a point of departure for reexamining conventional perceptions of national defense, strategy development, force projection, and force employment in the twenty-first century. Due to its relative intricacy—and critical assumptions—the following list summarizes key points detailed above:

- Information control is a *foundational requirement in peacetime and war*.

- *Information control* is now defined in terms of a strategy's informational requirements and involves freedom of access, maneuverability, and exploitation of an infosphere and the ability to prevent others from removing that freedom. Information control employs defensive capabilities for its attainment.

- Information control is achieved through controlling access to infospheres, achieved by first identifying and protecting assets in the physical dimension. The physical dimension includes the information collection and dissemination systems employed to enable a strategy, campaign, operation, and/or mission.

- *Information superiority* involves a relative condition of control—one side is able to control infosphere access as needed, while the opponent is not able to exert the level of control required by his strategy. While defensive capabilities are best suited for gaining and maintaining information control, offensive capabilities are optimized for gaining information superiority.

- An infosphere's physical dimension fundamentally consists of networked space and cyberspace systems. Thus, space and cyberspace control are now placed in context of information control (supporting controlled access to the infosphere),

and space and cyberspace superiority are necessary elements of information superiority.

- Integrated defensive space control and defensive cyberspace operations ensure protection of prioritized systems within the infosphere and thus contribute to the attainment of information control.

- Information control is a prerequisite for subsequent operations in all domains. Likewise, offensive space control and offensive cyberspace operations are best utilized *upon the attainment* of information control. Integrated offensive space control and offensive cyberspace operations are necessary for gaining information superiority.

- Assessing attainment (or loss) of information control and/or information superiority is convoluted and requires detailed analyses to establish appropriate criteria for verification. The "CIA Triad" of information security, consisting of information confidentiality, integrity, and availability may offer a model for devising information control metrics. Furthermore, these metrics collectively influence broad assessments of space and cyberspace control. This approach provides greater—and much needed—fidelity into the implications of degraded space and cyberspace capabilities on joint force activities across all levels (national to tactical).

- The higher probability of degradation rather than the complete denial of information systems creates an imperative for joint forces to develop a thorough and comprehensive understanding of how specific information systems (i.e., space and cyberspace) enable specific operations. Such integration would help strategists and warfighters recognize and anticipate the inflection points where reduced access to information drives adjustments to or even prevents operational activity.

- Information Age warfare will most likely create regions of strategic importance in space, cyberspace, or terrestrially that did not exist in previous conflicts. Adopting the new approach may help minimize unforeseen circumstances and may also help strategists understand the true capabilities, limitations, and susceptibilities inherent in their desired way of war.

- The scope, breadth, and depth of information control strategies warrant greater authorities and resources than currently allocated and expand far beyond the responsibilities given to geographic combatant commanders for IO (indeed, current notions of IO actually require proposed concepts of information control for their implementation). The Department of Defense should consider restructuring its forces to appropriately devise and orchestrate unified information control and superiority strategies for national defense.

- True transformation to Information Age warfare cannot occur (conceptually or operationally) without comprehensive acceptance and adjustment across the entire joint force. Similarly, modifications to space and cyberspace operations are not sustainable without comprehensive change at the joint force level and above.

The overarching concept of information control in the twenty-first century condenses accordingly. As discussed, Figure 7 illustrates the relationship between information, required force size, and precision firepower. The diagram illuminates an arbitrary region where the US military, and its political superiors, strives to conduct warfare. Furthermore, the illustration identifies notional inflection points where a certain loss of access to information will change the way the military can apply force (and whether force is even authorized given the additional risks imposed by a lack of precision). Thus, by combining the concepts presented in Figure 7 with the proposed methodology summarized above, a final synthesis follows: ***strategically, information control ultimately involves the ability to*** **recognize** ***and*** **prevent** ***degradation of infospheres that would lead to an undesirable retrograde in a particular strategy or way of warfare***. Additionally, ***information superiority denotes the ability to maintain such information control—relative to strategic needs—while eliminating the adversary's ability to recognize and prevent degradation of his own infospheres relative to his strategic needs***.

The final section captures key shortfalls in joint perspectives that must change to accommodate a comprehensive transformation to Information Age warfare.

Key Issues in Joint Perspectives

National and military strategies embody the prevailing viewpoints of national interests, national security, and the role of force. Military guidance derives its objectives from grand strategy and the various stages of its interpretation. When new strategies or challenges are expressed, the defense apparatus responds in ways that ensure organizational integrity remains intact. As Barry Posen noted, "Because each [military] service is concerned for its autonomy, a group of services is not likely to produce an agreed multi-service strategy or doctrine that does anything more than combine their

independent service doctrines."[57] Currently, joint forces and military services align themselves with recognized domains of land, sea, air, space, and cyberspace and seek to control the domains to create conditions that enable the security or projection of national interests. Establishing a national and/or joint information control strategy that transcends or challenges this construct will invariably generate strong reactions as to the proper command authorities and implementation of service capabilities and responsibilities.

The realities of Information Age warfare now confront current domain designations, particularly in the cases of space and cyberspace. The advent of cyberspace as a domain materialized alongside the recognized transition to the Information Age. As a result, although cyberspace does not hold a monopoly on information, cyberspace operations are now synonymous with Information Age warfare. In a domain-centric mentality, the preponderance of information operations thus falls to the cyberspace domain. On the other hand, space power, which arguably initiated the Information Age, currently retains its long-standing association with air power as related domains. As highlighted in the first section, this domain-oriented construct typically allocates responsibility for air *and space* superiority to the Air Force component commander, or COMAFFOR.[58] In each case, prevailing organizational structures and operational responsibilities for space and cyberspace directly counter the proposed methodology for information control.

Furthermore, information operations at the combatant command level are inadequate for managing information control strategies. The underlying (and implied) assumption driving IO structures, responsibilities, and activities is that a certain level of information control or superiority already exists by virtue of the superior information technologies available to national and military organizations. The employment of IO staffs, IO cells, and even JIOWCs—in conjunction with the CFACC's traditional responsibility for space superiority in theater—at the JFC level, without a central information control strategy, are a testament to this assertion. In sum, *the joint force is*

---

[57] Posen, 226.

[58] For example, during Operations Enduring Freedom and Iraqi Freedom (OEF / OIF), the theater COMAFFOR (in this case, dual-hatted as the CFACC) was given the task of gaining and maintaining air and space supremacy. See Benjamin S. Lambeth, *The Unseen War: Allied Air Power and the Takedown of Saddam Hussein*, (Annapolis, MD: Naval Institute Press, 2013), 20.

not focused on gaining and maintaining information control on a global scale and is therefore not postured for victory in the Information Age.

The premise returns to how the Department of Defense develops space and cyberspace infrastructures and whether their delineation prevents the advancement of information control concepts. While space and cyberspace technologies are inherently integrated from a systems perspective, their domain strategies and operations are not necessarily unified, creating a potential capability gap. In this sense, a contrast between *technology* and *capacity* provides insight into the true nature of this dilemma. Technology refers to the technical platforms (i.e., physical artifacts and software) and integrated systems that contribute to a particular function.[59] For the purposes of this analysis, *capacity* involves the larger infrastructure that enables or optimizes the planning and employment of a technology within a particular environment or context. One common joint model for describing an infrastructure's components is known as DOTMLPF (doctrine, organization, training, materiel, leadership, personnel, and facilities). Understanding the enabling and inhibiting factors of DOTMLPF on domain operations provides key insights into the implications of strategic change. Indeed, a 1996 report titled *The Unintended Consequences of Information Age Technologies* (requested by former CJCS, General John Shalikashvili) concluded that "changes in the flow of information [can] be dysfunctional if these changes [are] not also accompanied by changes to concepts of operation, doctrine, organization, command concepts, training, and other elements of a mission capability package."[60] Under these precepts, even if the Defense Department pursued a formal information control strategy, it is unclear whether existing space and cyberspace DOTMLPF are adequate for accommodating key aspects of information control presented in this chapter.

Conclusion

America's way of life and desired way of warfare are now contingent upon the availability of integrated space and cyberspace systems. The capacity for rapid communication, shared knowledge, and mass collaboration promote non-linear thinking,

[59] Merritt Roe Smith and Leo Marx, eds., *Does Technology Drive History?: The Dilemma of Technological Determinism*, (Cambridge, MA: The MIT Press, 1994), 102-103.
[60] Alberts et al., 50.

flexibility, and adaptability and are made possible through the existence of global communication networks built upon space and cyberspace technologies. Indeed, national prosperity and security in the form of worldwide power projection and force employment—ranging from diplomatic and economic influences to the viability of RPVs—now depend on assured *and combined* access to space and cyberspace.

If the United States intends to preserve its way of life and sustain its desired way of warfare in the twenty-first century, it must deliberately establish a comprehensive information control and information superiority strategy that precedes all other initiatives. In the Information Age, the convergence of space and cyberspace networks—separated by decades in their development—inadvertently formed the physical foundation of global and regional infospheres. Now, all national and international activities subsist under the physical and virtual umbrella of infospheres, relying on their global interconnectivity to collect and disseminate massive amounts of data to anyone, anywhere, at any time. Thus, in the pursuit of information control, an information control strategy should first focus on the identification (creation) and protection of the infospheres that enable particular operations. By extension, then, control of space and cyberspace (i.e., freedom of access, maneuverability, and exploitation, as dictated by strategy) sets the conditions for infosphere control and information control.

The joint force is currently not postured for this new approach to warfare. Combatant command authorities, roles, responsibilities, and resources are allocated based on a *regional*, domain-centric approach to operational control of contested environments. While incredibly useful, the conventional paradigm naturally separates the utility of space and cyberspace based on their physical and virtual characteristics. Joint doctrine does recognize the close relationship between space and cyberspace, but treats space capabilities more as expansions of air power than components of larger information architectures. On the other hand, cyberspace operations are perceived as the primary vehicle for IO and simply incorporate space as a consideration into their functionality. The new model re-categorizes space and cyberspace operations as functional equivalents in terms of information collection and dissemination (as they are interdependent) and aligns them under the framework of an information control strategy. In so doing, information control extends beyond geographic AORs and encompasses the globe. Thus,

the pursuit of information control requires a global presence and worldwide effort through the support of geographic entities. Such a structural change exceeds the scope of theater JFC authorities or capacities—information control is inherently a *global* fight.

In this sense, an information control strategy and subordinate campaigns are distinct from yet integrated with national and theater campaigns. Information control campaigns thus warrant their own organization, authorities, roles, responsibilities, and resources to plan, execute, coordinate, and assess information control activities in space and cyberspace. Elevating and prioritizing information control at the strategic and campaign levels also provides strategists and warfighters greater insight into the relevance of space and cyberspace systems to JFC campaigns or operations. From this standpoint, an information control campaign allows for the proper coordination, identification, and protection of critical space and cyberspace capabilities across the joint force and allows for the shared recognition of mission impacts due to specific information system degradation. Similar to John Warden's push for air superiority as a prerequisite for all other operations, information control and superiority now serve as precursors for all activities in peacetime and war. Such an approach demands greater oversight than currently provided.

Finally, even if the Department of Defense readjusted its forces to achieve and sustain information control at all levels, its capacity to do so at the operational and tactical levels remains in question. First, cyberspace operations are evolving and have yet to solidify into a universally accepted doctrine, let alone a domain definition. However, the lack of history in cyberspace may prove beneficial in forming a new paradigm for strategy and operations, as any transition is less profound. Conversely, space operations began in the 1950s and formed their own imbedded cultures over time. Legacy perceptions of space power, first established during the Cold War, prevail to this day and influence the space infrastructure's current DOTMLPF construct. Consequently, any transformation of space operations to the new information control model may encounter substantial inertia, *and traditional space policies and strategies may even inhibit the attainment of information control in future conflicts*. As indicated earlier, any accepted change to joint operations must occur at all levels and address a broader effort of national security. The information control paradigm is neither exclusive to the joint

force nor space and cyberspace operations—it is a national security issue. Thus, a unified acceptance of information control requires concerted efforts from the entire defense establishment and an investigation into its implications at the strategic, operational, and tactical levels.

The analysis now transitions to its second part with a broad investigation of the US space infrastructure's ability to achieve space control. Chapter 4 includes an examination of key events in US space history to build a basic understanding of the current culture surrounding space operations. The chapter closes with a review of the emerging threat environment, providing context for assessing the feasibility of long-standing policies and strategies. The overall analysis concludes in Chapter 5 by advocating for a space control strategy under the premise of information control. Space DOTMLPF structures are presumed inadequate for the Information Age warfare requirements presented here, and recommendations are provided for transformation, as applicable.

Chapter 4

US Space Operations—History, Culture, and Emergent Threat Environment

To learn and change, organizational members must be skilled in understanding the assumptions, frameworks, and norms guiding current activity and be able to challenge and change them when necessary.

- Gareth Morgan

[The threat of invasion over land] pointed to a more fundamental reason for [China's] official abandonment of overseas ventures. A formidable and feared enemy existed across the land frontier, whereas, until the rise of 'Japanese' piracy in the late fifteenth century, there was no rival on the seas with whom the Chinese had to fear.

- William H. McNeill

The use of space to serve society's needs had undergone a transition from luxury to necessity.

- William E. Burrows

The Industrial and Information Ages are best differentiated by how humans perceive and attempt to manipulate the world around them. Notions of prosperity and security stem from each paradigm's underlying assumptions, formulating accepted norms, influencing behavior, and characterizing problem-solution sets. In the case of the Industrial Age, problems and solutions were framed by a belief in the viability of structure and stability. In the Information Age, problems and solutions are viewed more in terms of circumstances and relationships and are thus more situation-dependent.[1] By and large, the US military organizes and employs its forces based on traditional concepts sustained through the Industrial Age. While the United States still wields the most formidable military in history, evolving strategic landscapes and the rise of Information Age precepts create engagements that are not always conducive for industrial age methods.

The compartmentalization of physical and virtual domains, discussed in Chapter 3, serves as a useful illustration for the US military's traditional approach to force application and control. Under traditional thinking, land, air, maritime, and space domains are separated from cyberspace by both medium and function. Although joint

[1] John E. Rothrock, Edward F. Smith, Jr., and John F. Kreis, *The Industrial Age Versus the Information Age: Rethinking National Security in the 21st Century*, IDA Document D-2536 (Alexandria, VA: Institute for Defense Analyses, 2001), 10.

forces seek full-spectrum superiority through cross-domain operations, domains serve as useful structures for assigning authorities, roles, and responsibilities (i.e., organizing, training, equipping, and operating). Furthermore, services and components provide expertise on how best to control access and exploit their respective domain.

However, the modern appreciation of complexity, non-linear relationships, flexibility, and agility transcends conventional boundaries and instead views interactions through adaptive networks. Under the new paradigm, space capabilities—traditionally compared with air operations—are considered part of a larger, global, and more complex information collection and dissemination network, enhanced by cyberspace capabilities. In this regard, the shift in warfare presented in Chapter 3 proposed a re-categorization of space and cyberspace as complementary domains based on their functional relationship. Collectively, space and cyberspace form the backbone of infospheres—the physical and virtual structures that collect and disseminate global, near real-time, and accessible information—and thus create an environment that allows for non-linear reasoning. If the United States seeks to preserve its prosperity and security in the information age, it must rethink how it perceives traditional demarcations in military organization and force employment; and it begins with space and cyberspace.

Organizational transformation is difficult and may in fact prove detrimental if done incorrectly or motivated by false pretenses. As Gareth Morgan observed in the chapter's opening comment, effective change cannot truly take place without first understanding the prevailing conditions that shaped the current organizational culture. Only then can groups recognize procedural or conceptual aspects that no longer accommodate the new landscape and respond accordingly. Likewise, adaptation is futile, even counterproductive, without a guiding vision or strategy to frame it. In this sense, the first three chapters fashioned a broad vision for change. Thus, the final two chapters examine institutional and organizational culture in the US military, specifically from the perspective of space operations. The US space infrastructure provides an excellent opportunity to assess prevailing perspectives in the military for two key reasons. First, because the US space culture formed over the course of several decades, it holds greater inertia than the cyberspace culture, which is still seeking its own identity. As a result, the US space culture is more representative of the broader defense mindset and serves as a

model for evaluating the joint force's requirements and capacity for adaptation. Second, space operations constitute a central component of information control, compelling the joint warfighting community to understand the possibilities and obstacles associated with gaining information control through prevailing notions of space operations.

The analysis thus continues with a review of key events and timeframes in the US space program's history that shaped present conditions. The chapter concludes with a brief description of the emergent threat environment in space, providing additional context for final analysis in Chapter 5. Despite recent rhetoric and political positioning to the contrary, the US military plans and operates as though space is an inherently permissive environment and is therefore not postured to enable information control given the emerging strategic landscape.

Historical Context and Current Military Space Culture

The US space program's history is rich with stories that portray examples of creativity, intrigue, suspense, accomplishment, failure, apathy, commitment, change, and surprising timidity. Indeed, to fully internalize the totality of the US space experience requires a separate investigation. However, a review of six events and historical timeframes produces a sufficient story that explains the modern space culture (broadly covering strategic context, international law and policy, and organization). These events include the Soviet launches of *Sputnik I* and *II* (and the US reaction); the dawn of space-based strategic reconnaissance; the implications of The Outer Space Treaty of 1967; the maturation of military space from the 1960s to 1980s; Operation Desert Storm and the concurrent collapse of the Soviet Union; and the institutional adjustments that took place after the end of the Cold War.

The Sputniks

The world changed on October 4, 1957. Mankind's curiosity, imagination, and ingenuity culminated in one singular event: the launch of *Sputnik*, the first man-made object to orbit the earth. The feat, achieved by the Soviet Union, sent shockwaves across public and political realms, and speculation as to its implications on society's future consumed discourse in all sectors. Significantly, the sudden transformation of space

travel from fiction to reality occurred at a most precarious point in history. The Cold War served as a tense backdrop for the monumental event, manipulating perceptions of *Sputnik's* relevance to human affairs. All reactions emerged from the context of nuclear deterrence and ideological supremacy, two mainstays of Cold War competition. Contemporary and historical accounts are almost unanimous in describing the situation as a "crisis," both in terms of US national confidence and geopolitical ramifications around the world.[2]

From a Cold War perspective, the launch of *Sputnik* ushered in a new dimension of national security considerations. Overnight, communist Soviet Union gained a decided advantage over the liberal democracies in the free world. In one sense, *Sputnik's* success portrayed the Soviet Union as an incredibly sophisticated and technical society, perhaps even more so than the United States. Of greater concern, however, was how the Soviet Union's sudden—and exclusive—access to space placed the United States in a precarious geopolitical position, primarily for two reasons. First, the reality of the Soviet Union's accomplishment established a new battleground for competition. The United States and Soviet Union subsequently pursued space "as a 'new high ground' that must not be abandoned to the other."[3] As then Senate Majority Leader Lyndon Johnson proclaimed, "The urgent race we are now in . . . is not the race to perfect long-range ballistic missiles, important as that is. There is something more important than any ultimate weapon. That is the ultimate position—the position of total control over Earth that lies somewhere out in space."[4]

From a national security standpoint, and despite Senator Johnson's assessment, the second issue dealt with the natural technology transfer between a space launch vehicle and a ballistic missile. The Soviet Union's successful insertion of a satellite into orbit simultaneously revealed the capacity to rapidly deliver a nuclear warhead to any point on the globe. The United States had no defense against such a weapon, making

---

[2] Philip Taubman, *Secret Empire: Eisenhower, the CIA, and the Hidden Story of America's Space Espionage*, (New York, NY: Simon and Schuster, 2003), 212.; Roger D. Launius, *NASA: A History of the U.S. Civil Space Program*, (Malabar, FL: Krieger Publishing Company, 1994), 17.
[3] Launius, 17.
[4] William E. Burrows, *This New Ocean: The Story of the First Space Age*, (New York, NY: The Modern Library, 1998), 189.

"the leader of the free world vulnerable to annihilation for the first time."[5] To add insult to injury, while the Americans were still coming to grips with *Sputnik's* implications, the Soviet Union successfully launched a much larger satellite, *Sputnik II*, on November 2, solidifying Soviet superiority in rocket technology. The culminating point came in the closing weeks of 1957 when journalist Chalmers Roberts unearthed the classified Gaither report. The report concluded the United States was "in the gravest danger in history" and described "an America exposed to an almost immediate threat from the missile-bristling Soviet Union."[6] This declaration, along with others like it in the report, established the basis for a purported "missile gap" that would haunt US decision makers and challenge intelligence collection and analysis across the entire defense apparatus for several years.[7]

The fallout from the *Sputniks* was not entirely oppressive, however. Prior to the advent of space travel, the United States sought "freedom of space" as an international norm but had no way of advancing its position, particularly among nations who lacked the technical and industrial capacity for spaceflight. The *Sputniks* inadvertently paved the way for international acceptance of satellite overflight—neither satellite incited a single diplomatic protest.[8] Donald Quarles, then deputy secretary of defense, believed the Russians had done the United States a favor by effectively confirming national boundaries—and national air space—did not extend into outer space. Satellite overflight thus did not infringe on national sovereignty, normalizing freedom of space as an international policy, thereby paving the way to legally send spy satellites into orbit.[9] Most fortuitously, freedom of space emerged at a time when President Eisenhower faced the almost insurmountable burden of stabilizing relations with the Soviet Union while maintaining persistent awareness of their nuclear capabilities. Space-based reconnaissance provided a means to do both.

Until October 4, 1957, humans had fantasized and speculated about the seemingly endless possibilities of space exploration and exploitation. In reality, after the *Sputniks*,

---

[5] Burrows, 190.
[6] Taubman, 274.
[7] Taubman, 275, 277.
[8] Delbert R. Terrill, Jr., *The Air Force Role in Developing International Outer Space Law*, (Maxwell Air Force Base, AL: Air University Press, 1999), 30.; Launius, 27.
[9] Burrows, 187.

the US and Soviet space programs arose under the foreboding confines of Cold War politics. A narrowly focused scaffold was set for the developing space culture.

Space-Based Strategic Reconnaissance

The concept of strategic reconnaissance did not result from *Sputnik*. However, access to space redefined connotations, possibilities, and expectations of strategic reconnaissance, particularly during peacetime. In 1946, Richard Leghorn, then a pilot in the US Army Air Force, revised his perceptions on war while conducting aerial reconnaissance operations at Bikini Atoll in support of nuclear weapons testing. In one underwater test, termed *Baker*, old warships were thrust into the air as though they were plastic toys, and eight of them eventually sank after falling back to the surface. To Leghorn, the consequences of war changed in an instant: "I knew at that moment we couldn't have another war," he later recalled.[10]

Leghorn was motivated by the possibility of preventing a surprise nuclear attack against the United States. He pondered ways to gather better intelligence to aid decision makers in anticipating Soviet activities and deterring hostile action. In this endeavor, Leghorn believed that military intelligence had to *consistently* monitor military forces and industrial facilities and brief the White House and Pentagon on a recurring basis. In similar fashion, the year prior, General Henry "Hap" Arnold acknowledged that Washington needed "continuous knowledge of potential enemies," which included their "political, social, industrial, scientific, and military life."[11] Leghorn concluded that the United States should embark on continual peacetime reconnaissance operations over the Soviet Union. The challenge, of course, was collecting such intelligence without provoking war, particularly since national sovereignty extended into the airspace above internationally recognized borders.[12] "It is extraordinarily important," he announced in 1946, "that a means of long-range aerial reconnaissance be devised *which cannot be detected*" (emphasis added).[13]

---

[10] Taubman, 36-37.
[11] Taubman, 40. In many respects, General Arnold's conception of strategic intelligence illustrates the basis of modern IPOE endeavors in the pursuit of an operational environment's PMESII (see Chapter 3 of this thesis).
[12] Terrill, Jr., 1.
[13] Taubman, 39.

Leghorn's vision eventually manifested itself in the legendary U-2 spy plane, a mainstay of US strategic reconnaissance operations during the mid-1950s (and a system still employed today). At its inception, the U-2 was able to travel long distances and attain altitudes that Soviet air defenses could not intercept. However, President Eisenhower routinely proved reluctant to employ the system, particularly in 1956 as relations with the Soviet Union appeared to warm. When authorized, though, U-2 missions collected invaluable information on Soviet nuclear capabilities. As time progressed, and as air defense technologies improved, Soviet protests of U-2 infringements intensified. Thus, lingering fears of aggravating the Soviets prompted President Eisenhower to keep the operations secret from the public. Meanwhile, advancements in radar and interceptor technologies increasingly brought the Soviet Union closer to successfully engaging U-2 flights over their airspace.

By 1959, Eisenhower's concern of Soviet retaliation forced him to limit U-2 missions considerably. All U-2 flights required authorization from the president, and he granted permission sparingly. The trade-off created gaps in reconnaissance of Soviet activities, and the newfound fears of ballistic missile technologies—spawned by the *Sputniks*—created an even greater dilemma. At the same time, both countries now enjoyed free access to space, and Eisenhower pressed the Pentagon and Central Intelligence Agency (CIA) to deliver a spy satellite that could bridge the intermission between the U-2's grounding and employment of its planned replacement, the A-12 Oxcart.

Prior to the *Sputniks*, the USAF initiated work on a spy satellite that would collect intelligence and transmit it back to earth via television signals. The project was named WS-117L and incorporated an ambitious design, one that exceeded existing technical capacities (indeed, the United States had yet to successfully insert a satellite into orbit). By the start of the space age in 1957, several other satellite designs were under consideration in the United States. All systems were "designed to break out of the electronic straitjacket of ground communication by relaying messages around Earth from the high vantage point of space."[14] As pressures mounted for creating a persistent strategic reconnaissance platform—something the U-2 could not provide even if it was

[14] Burrows, 225.

employed regularly—the Pentagon and CIA sought ways to exploit more feasible technologies already in development. Consequently, the United States shifted focus from the WS-117L's television-based design to a more achievable, yet still challenging, photoreconnaissance satellite that would take photographs and jettison the film in a recoverable capsule back to earth. In a fortunate turn of events, Richard Leghorn, now a member of the Aerial Inspection Subcommittee of the President's Arms Control and Disarmament Group, reentered the scene to help design and produce the revised spy satellite.[15] The new satellite, named *Corona*, marked the dawn of space-based reconnaissance and effectively set US space operations in motion.

From a cultural standpoint, the most noteworthy aspects of *Corona* came in the forms of program authority, tasking, and secrecy. As noted, the WS-117L fell under USAF (i.e., military) purview. However, Eisenhower emphatically directed that *Corona* was a CIA program and that all other governmental agencies would support the CIA in its endeavor. Thus, the Pentagon offloaded its technical expertise gained through the WS-117L and ceded its control of the program. Additionally, due to reasons of national security in the realm of Cold War politics, the *Corona* project was wrapped in suffocating secrecy. To preserve confidentiality during its development, the government devised a strategic narrative to convince the world that the WS-117L—and its mission—was shelved. Furthermore, the cover story insisted the Air Force was instead pursuing a scientific satellite, called *Discoverer*. Journalists, and the Russians, would believe the United States no longer intended to develop a spy satellite. The Air Force proceeded with building a launch site under cover of the *Discoverer* story.[16] In August of 1960, the site launched the first fully operational, and highly secretive, *Corona* satellite into orbit.

The year 1960 marked a significant turning point in strategic reconnaissance, information, and space culture. By that time, the Soviet Union fielded a highly sophisticated and capable air defense system and successfully shot down a U-2 spy plane piloted by Francis Gary Powers. In an ironic turn of events, on August 19, 1960, the Soviet Union convicted Gary Powers of espionage. The very same day, unbeknownst to the Russians, *Corona* collected the first photograph of the Soviet Union taken by a

[15] Taubman, 228.
[16] Taubman, 239.

satellite, marking the commencement of the largest intelligence collection campaign in history.[17] Although not fully appreciated at the time, an entirely new dimension of strategy was born as *Corona* sparked the implementation of the first global, persistent information collection and dissemination network used for decision-making. Most notably, space operations commenced under the authority and expertise of the US intelligence community—led primarily by scientists and engineers—and were designed to collect and disseminate information *from* space, setting the framework for future mindsets.

The Outer Space Treaty

After World War II (and prior to the *Sputniks*), desires to prevent space from succumbing to the inevitability of human conflict drove the scientific and legal communities to limit military competition in the domain. In 1919 and 1944, international conventions acknowledged that state sovereignty included the airspace above national territory. However, neither convention identified where outer space began, and thus the issue on whether sovereignty included the space domain was not addressed. For those determined to seclude space from terrestrial strife, the delineation of airspace and outer space proved immensely important. John Cobb Cooper, an early advocate for the sanctity of space, drafted a treatise in 1951 titled "High Altitude Flight and National Sovereignty," sparking intense debate on the necessity to distinguish the space domain from air.[18] The absence of international dispute against the *Sputniks* all but confirmed that state sovereignty did not extend into outer space, leaving an open door for demarcating the region.

Rather than clearly identifying outer space and isolating it from the throes of combat, however, the United States and Soviet Union initiated vigorous campaigns to secure access and dominate the domain. Although President Eisenhower pursued an Open Skies policy and sought freedom of access to space, Cold War pressures brought a dose of reality to the situation.[19] By the time President Kennedy took office, the strategic

[17] Taubman, 321.; Burrows, 221.
[18] Terrill, Jr., 1-2.
[19] President Eisenhower's "Open Skies" proposal was designed to "soften the transition to the missile age" by establishing a cooperative relationship with the Soviets that allowed for transparency via inspection

tension had thickened and a consuming, almost incessant attraction (or capitulation) to the inevitability of nuclear warfare permeated political and military thought. Space was not immune to warfare, and in fact offered a key position for nuclear conflict, particularly from the standpoint of reconnaissance and communications.[20] Prompted by a belief that control of space was essential in a future world war, the US government conducted a series of exo-atmospheric nuclear tests, labeled Project Fishbowl. On July 9, 1962, US scientists initiated *Starfish Prime,* a nuclear test that detonated a 1.4-megaton warhead at an altitude of approximately 250 miles. The nuclear explosion degraded radio transmissions from California to Australia for several hours and eventually incapacitated six satellites on orbit.[21] Similarly, the Soviet Union deployed several nuclear-tipped anti-ballistic missiles—capable reaching altitudes attained in the *Starfish Prime* test—in the same time period.

By the time *Starfish Prime* commenced, the Space Age was only four years old. Nevertheless, in those four short years, both the Soviets and Americans had fielded ICBMs, conducted multiple high-yield nuclear tests, and continued investing heavily in military space programs. Despite the Soviet Union's initial success in space, the United States soon surpassed its presence in the domain, and the Soviet command economy was not yet primed to regain the lead. The best option available to Russian Premiere Nikita Khrushchev at the time was to vehemently protest US military activities in space, particularly its reconnaissance efforts. Nonetheless, while Soviet rhetoric lambasted US reconnaissance initiatives and its overall "militarization" of space, it also implicitly endorsed the potential of space-based weaponry. In fact, the majority of Soviet publications heralded the certainty of Soviet dominance in space and highlighted its economic rewards as a national imperative.[22] Thus, Soviet objections attempted to

---

flights over each other's territory and offered "blueprints of all bases and armed forces." Russian Premiere Nikita Khrushchev disagreed on the belief that "Open Skies" was a deceptive method for espionage. For further reading, reference Walter A. McDougall, *The Heavens and the Earth: A Political History of the Space Age*, (Baltimore, MD: The Johns Hopkins University Press, 1985), 127.

[20] By 1962, the United States had already launched 63 payloads, 34 of them belonging to the military. The Soviet Union, on the other hand, had only launched 15. However, both programs soon attained a relative level of parity, eventually forcing decision makers to pursue bilateral and multilateral agreements in space law. See McDougall, 272.

[21] James Clay Moltz, *The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests*, (Stanford, CA: Stanford University Press, 2008), 119.

[22] McDougall, 270-271.

temporarily neutralize America's newfound advantages and bide time for Soviet expansion. Ultimately, the Soviet position manifested itself in the international space treaties that followed.

Fallout from US and Soviet nuclear testing extended beyond atomic radiation. The unexpected consequences of the high altitude blasts, coupled with heightened competition and political posturing to leverage (or deny) control of the domain, eventually led to a series of agreements between the nuclear superpowers not to conduct nuclear weapons testing in the atmosphere, in outer space, or underwater. The first significant agreement, codified in the Limited Test Ban Treaty of 1963, marked a unique milestone in the Cold War standoff and set the stage for a series of subsequent arms control treaties that appeared intent on cooperation, particularly in space. For example, in successive treaties, both sides agreed to refrain from placing nuclear weapons in orbit, and the Soviet Union finally rescinded their exhaustive protest against US space-based reconnaissance efforts.[23] However, one common view of the treaties, articulated by Charles Duelfer, suggests the initiatives were more calculated: "The U.S. and U.S.S.R. generally agreed to ban things they were not going to do anyway. On weapons they did want, they agreed to numeric ceilings that were so high that they go to do everything they wanted."[24] Indeed, as the 1960s progressed, nuclear arsenals on both sides exploded to obscenely large numbers, and—along with further expansion of space capabilities—ultimately forced policymakers back to the negotiating table in 1966 and 1967 for another monumental arrangement.

During the Kennedy Administration, and prior to the test ban treaties of 1963, the United States officially declared that all US space programs—civilian *and* military—existed for peaceful purposes.[25] The policy served to rebuff the self-serving Soviet complaints of US space endeavors (indeed, the Soviets routinely contradicted their publicized views of demilitarizing space in doctrine and practice) and set the conditions for treaties to follow. As a result, the concept of "sanctuary" drove US military space

[23] McDougall, 274. Additionally, by 1963, the Soviets started fielding their own reconnaissance satellites and were thus willing to cease their diplomatic objections to US activity in space. (See McDougall, 348.)
[24] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It*, (New York, NY: Harper Collins, 2010), 221. Charles Duelfer was a leader of the UN team established to curtail Iraqi WMD efforts during the 1990s.
[25] McDougall, 335.

policy for decades, and still underscores US and international space programs (and policy debates) today. The notion of space as a sanctuary persisted in large part due to the continued acceptance of the United Nations Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies—or simply The Outer Space Treaty (OST)—of 1967. Of note, the treaty officially went into effect on October 10, 1967, just over ten years after *Sputnik's* historical voyage. The OST, hailing notions of space as a sanctuary and the "province of all mankind," ultimately resulted from the combination of human aspirations and the calculated political waltz that moved to the rhythm of Cold War dynamics.[26]

Two opposing—and widely held—views of the OST's implications persist today. The first is that it stifled incentives for space expansion and emerged as a result of Cold War blustering. Additionally, the first view suggests that the OST, while internationally recognized, catered more to the Soviet perceptions of space in context of possible US supremacy (and, therefore, a loss of Soviet dominance). As Dr. Everett Dolman maintained, "The Outer Space Treaty, as it was eventually penned, would prove to be more of a modification of the Soviet view than of the US view."[27] The critique echoed a prevailing response during the period, as journalists of the time retorted that the space treaties up to and including the OST essentially restricted the employment of technologies already considered unfeasible. Moreover, the OST technically did not restrict the placement of weapons on orbit—it only outlawed the deployment of weapons of mass destruction in the domain. Therefore, *any* "space treaty could only be a façade to make the Cold War rivals look good without constraining them from doing anything they might really want to do."[28] The OST essentially captured the US and Soviet concerns that had emerged over the past several years, but it also restricted (and even discouraged) private interest and commercial expansion, stagnating space innovation and relegating space norms as a balance for great power rivalries.

---

[26] For a list of the provisions outlined in the OST, reference: US Department of State, "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies," 27 January 1967, http://www.state.gov/t/isn/5181.htm (accessed 13 November 2014).
[27] Everett C. Dolman, *Astropolitik: Classical Geopolitics in the Space Age*, (London, Frank Cass, 2002), 124.
[28] McDougall, 416.

The second, more fantastical view suggests that the OST actually represented an exemplar of human cooperation. In a time of intense geopolitical tension, the OST brought together the nations of the world and articulated a common sentiment that served as a beacon of hope. As observed by space lawyers Glenn Reynolds and Robert Merges, "The [OST] can be said to represent a more general view of the interests of humanity instead of being merely a compromise among interested parties, shaped primarily by the balance of power."[29] While evidence suggests this was not the case, at least under the surface, a large contingent of analysts and arms control advocates perceive the OST in this regard and refer to its ratification as a milestone in international relations. Regardless of its original intent, however, the OST continues to inform—and even entice—debates about the proper exploitation of space for national security and international cooperation.

In the end, the first interpretation of the OST's context appears more explanatory. The OST did not eradicate military use of space, prevent space-based reconnaissance operations, or even ban the deployment of conventional weapons in the domain. Although the OST promulgated the perception of space as a sanctuary, the Soviet Union and United States *still expected to fight in space* if they engaged in war against one another. Their mutual militarization of space in the years following the OST is a testament to this fact.

The Maturation of Military Space

Military involvement in space grew significantly between the 1960s and 1980s, all under the structure of nuclear deterrence and nuclear warfare. As the US intelligence community continued with the prioritized mission of strategic intelligence, the US military slowly formalized its role in the domain. Over the course of several decades, the US military developed advanced missile warning, space surveillance, satellite communications (SATCOM), weather, data relay, reconnaissance, launch, and navigation capabilities and networks that continue to define its function in space today. Ultimately, by the 1980s, the evolution of national and military space strategy led to the formation of

[29] Quoted in Michael Moore, *Twilight War: The Folly of U.S. Space Dominance*, (Oakland, CA: The Independent Institute, 2008), 6.

two principle organizations: Air Force Space Command (AFSPC) and United States Space Command (USSPACECOM), both of which experienced continual change and upheaval in the years following their inception.

After its initial forays into space-based reconnaissance (i.e., the WS-117L), the Department of Defense began construction on a ground-based missile warning architecture that could detect and track inbound Soviet ICBMs. The architecture, eventually known as the Ballistic Missile Early Warning System (BMEWS), fulfilled two missions, both new disciplines in the military's catalog of expanding capabilities: strategic missile warning and space surveillance. In the early 1960s, the initial BMEWS architecture consisted of globally distributed sites in Greenland, Alaska, and England. Development of exclusive space surveillance systems occurred shortly thereafter, including radar and optical technologies. The combination of BMEWS systems and space surveillance sites formed a robust, global network of tracking capabilities designed to provide near-instantaneous situational awareness for decision-makers in a nuclear environment.

As the 1960s continued, ballistic missile technology and space capabilities continued their unremitting advancement. The Soviet Union and United States began fielding submarine-launched ballistic missiles (SLBMs), shortening detection and warning timelines and forcing the deployment of more sophisticated warning networks. Additionally, by 1965, the Soviet Union was launching nearly *twice* as many spy satellites as the United States.[30] At the same time, SATCOM technologies exploded, and more satellites filled orbital space. In 1962, *Telstar*, the first commercially funded communication satellite, provided telephonic communications between the United States, Great Britain, and France. The following year, National Aeronautics and Space Administration (NASA) launched *Syncom*, the world's first communications satellite in geosynchronous orbit, capable of transmitting a wide range of signals to a much broader audience.[31] As discussed in Chapter 2, 1965 saw the dawn of international SATCOM

[30] McDougall, 272.
[31] *AU-18 Space Primer*, (Montgomery, AL: Air University Press, 2012), 11. Of note, the term *geosynchronous* refers to a unique orbit whose period matches the earth's rotation, giving it a relatively static position over a pre-determined spot on earth. The orbital altitude of approximately 22,000 miles also offers an opportunity to provide greater coverage of the earth—one antenna on a satellite in geosynchronous orbit can cover nearly one-third of the earth's surface.

ventures in the activation of INTELSAT I. Furthermore, in 1968, the Soviet Union activated *Molniya*, the first high-altitude Soviet communication satellite designed to deliver continual SATCOM coverage of the Soviet mainland. The proliferation of space-related technologies demanded greater oversight from the defense apparatus, and the US and Soviet militaries responded accordingly.

The nuclear arms race held a symbiotic relationship with the militarization of space. As ICBM and SLBM technologies improved and arsenals expanded beyond reason, a more comprehensive warning capability was necessary. Space offered a unique vantage point for collection and dissemination of missile launches, and both sides deployed space-based missile warning systems—primarily exploiting the infrared (IR) portion of the EMS—to detect and characterize strategic missile launches in a matter of seconds. Secure communications were also needed for command and control of nuclear forces in response to hostile missile launches, and military SATCOM capabilities were developed to fulfill this role. Furthermore, preliminary space-based IR systems could not adequately detect heat signatures through clouds, and therefore weather prediction became increasingly important. As a result, weather satellites such as TIROS (Television Infrared Operational Satellite—no longer employed) and the Defense Meteorological Satellite Program (DMSP), first launched in 1962, provided general and mission-specific data collection on terrestrial weather in support of missile warning and other national defense endeavors.

In addition to missile warning, nuclear C2, and weather, robust communication networks were required to maintain control of critical on-orbit systems and increase awareness of activities in the space domain. Ground-based satellite command and control architectures soon spread across the globe to ensure constant vigilance of space-based systems. Moreover, in addition to deploying a modernized tracking capability for missile launches, the US expanded its space surveillance architecture to track and catalog the growing number of objects (civil, commercial, and military) in orbit. Collectively, the integration of ground-based missile warning and dedicated space surveillance sites produced the basis for the US Space Surveillance Network (SSN). In essence, the US and Soviet militaries constructed global, space-based information networks that provided near-real time information collection and dissemination for decision-making—all under

the umbrella of nuclear deterrence. Table 1 lists examples of early military space-related systems and associated missions that persist today—*all of which are inherently informational*.

Table 1: Early US Space-Related Missions, Systems, and Year First Fielded

Mission	Satellite / System[32]	Year(s) First Fielded
Missile Warning	- BMEWS (ground-based) - Defense Support Program (DSP) (space-based)	- Early 1960s - 1970
SATCOM	- Defense Satellite Communications System (DSCS)	- 1971
Weather	- DMSP	- 1962
Space Surveillance	- Space Surveillance Network (SSN)	- Early 1960s
Satellite C2	- Air Force Satellite Control Network (AFSCN)	- 1960s

Source: Author's Original Work

As the 1970s unfolded, the geopolitical environment remained tense, and military involvement in space continued within the confines placed upon it by international treaties and national policies. While the two sides pursued cooperative efforts in the civil sector, US and Soviet military posturing remained focused on controlling access to the domain in the event of hostilities. This perception of space emerged from a prevailing (and somewhat mutual) perspective that the space domain was a natural extension of the air, and that air operations logically transitioned into military space. As discussed, in 1958, General Thomas White—then Air Force Chief of Staff—commented, "In speaking of control of air and the control of space, I want to stress that there is no division, per se, between air and space. Air and space are an indivisible field of operations."[33] General White's perspective provided the impetus for merging air and space operations under a homogeneous *aerospace* domain. In 1975, in a then classified USAF report titled "New Horizons II, Volume V: The Role of the Air Force in Space," USAF strategists

[32] Due to the Soviet Union's approach to secrecy, all early space programs—regardless of mission—were named under the cover of *Kosmos*, and are thus not listed in tablature format. See McDougall, 272.
[33] Donald Cox and Michael Stoiko, *Spacepower: What it Means to You*, (Philadelphia, PA: The John C. Winston Company, 1958), 122.

articulated a similar view: "Based on the 'aerospace' concept, the Air Force has recognized that its vital role in this fourth medium [space] is a logical extension of air operations."[34] Consequently, military operations in space progressed from an enduring notion of warfare in the terrestrial environments (this approach also helped spark a series of subsequent debates, narrowly focused in their scope, on the weaponization of space).

The Soviet Union also viewed space as an essential element of a control doctrine in nuclear war. As indicated, the Soviets pursued similar space-based capabilities as the United States but employed diplomatic pressures and strategic narratives to impede US actions and portray US intensions as aggressive. Indeed, space-based reconnaissance, strategic missile warning, SATCOM, weather, and space surveillance capabilities all directly contributed to Soviet nuclear strategy. Furthermore, the Soviets independently developed offensive capabilities and doctrine with the intention of negating US advantages in and through the domain. For example, in 1967 (the year the OST was signed), the Soviets tested their infamous fractional orbital bombardment system (FOBS), which included a series of nuclear-tipped ballistic missiles that would enter low earth orbit (LEO) and de-orbit at a pre-determined time and place over the United States (typically from a southerly direction up from Antarctica and over Mexico).[35] The same year, the Soviet Union tested a series of maneuverable satellites "for inspection and destruction of hostile spacecraft."[36] Of note, the two Soviet examples highlight two very distinct concepts of space weapons—the first designed to exploit space as a high ground for terrestrial attacks and the second intended to gain control of the domain through offensive action against adversarial space-based capabilities. Both sides viewed the combined offensive capabilities as essential for winning a nuclear war.

The US military intended to counter Soviet aggression and ensure access to critical capabilities in support of nuclear deterrence and nuclear warfare. In the classified New Horizons II report, USAF strategists concluded that the "USSR has displayed a strong interest in the use of space for military purposes. The USSR is the first . . . nation

---

[34] Robert M. Camron, et al., *New Horizons, Volume V: Role of the Air Force in Space*, (Washington, DC: HQ USAF, 1975), xiii. Document is now declassified.
[35] Moltz, 156.
[36] McDougall, 273.

to develop strategic orbital offensive and defensive weapons."[37] Consequently, the USAF investigated the feasibility of terrestrial and orbital counterspace (or *counteraerospace*, as it was then termed) capabilities. The report advocated for the acquisition of an anti-satellite (ASAT) capability as well as associated upgrades to the surveillance network that could "detect, track, and identify objects in space out at least geosynchronous altitude."[38] The report further explored the feasibility of conventional space-based weapons that could target terrestrial military forces (a subject of intense debate and the primary focus of modern arms control activists who seek to eliminate weapons from space). In all, the report stressed that "the Air Force [must] vigorously pursue the acquisition of space systems to achieve the preferred military capabilities . . . in order to 1) enhance the effectiveness of [the US] strategic nuclear deterrent and its underlying essential equivalence and 2) capitalize on the inherent force-multiplier qualities of space systems to improve the ability of tactical forces to react quickly and efficiently on a global basis while minimizing dependence on overseas basing."[39] In the end, due primarily to technical and economic limitations, neither country deployed a fully operational counterspace architecture in orbit, but the concept continued to influence respective space strategies.

From the US perspective, the maturation of military involvement in space demanded a formal organizational structure for organizing, training, and equipping its forces. Furthermore, the reality *and acceptance* of space warfare drove requirements for a global warfighting command that could plan and execute strategic objectives in and through the space domain. As a result, the USAF first established Space Command as a major command (MAJCOM) in 1982 with the purpose of consolidating its missile warning and surveillance missions under one authority.[40] The new organization adopted personnel from Strategic Air Command (SAC) and Air Force Systems Command and soon increased its purview to satellite operations (including satellite C2) through the development of a Consolidated Space Operations Center (CSOC) at Falcon Air Force

[37] Camron et al., 2-4.
[38] Camron et al., xv.
[39] Camron et al., xvii.
[40] US Air Force Space Command, *Air Force Space Command Almanac 2004-2005*, (Peterson AFB, CO: HQ Air Force Space Command, 2005), 4.

Base, Colorado (now Schriever Air Force Base).[41] By 1985, President Reagan had articulated his Strategic Defense Initiative (SDI), which called for an intricate, expensive, and technically challenging network of missile defense capabilities that would eradicate the Soviet Union's ability to win a nuclear war. The Reagan Administration's approach to the Cold War standoff, combined with the military's growing space infrastructure, convinced the Pentagon to create a unified command *with the explicit purpose of controlling access to space*. United States Space Command (USSPACECOM) was thus formally activated in 1985, while Space Command was renamed Air Force Space Command (AFSPC) and given its service responsibility of organizing, training, and equipping USAF forces for the joint fight.

Throughout the entire period, the US intelligence community (IC)—by now a veteran and bedrock of US space operations—continued to mature its processes and capabilities under the cloak of extreme secrecy. Although the US military's role in space increased considerably, it joined a cadre of engineering and science professionals who perfected an *intelligence-centric tradecraft* that would continue to underscore all operations in the domain.[42] Furthermore, as the US military pursued ways for gaining space control, the intelligence community was postured to deliver intelligence from space rather than *for* space. The two cultures maintain different perspectives and priorities today, creating a unique dichotomy in the space culture. Nevertheless, by the end of the 1980s, the United States boasted a potent, expansive, and robust space infrastructure, and the world was about to witness the full potential of integrated operations on the modern battlefield.

1991: The Pivotal Year

The success of Operation Desert Storm and the Cold War's abrupt end sent decades worth of policy, strategy, and worldviews into chaos. As discussed in Chapters 1 and 2, the year marked a definitive turning point in national security, and no other entity in national defense experienced a more profound shift than the space community. The visible realization of space capabilities as force multipliers set the US space infrastructure

---

[41] Benjamin S. Lambeth, *Mastering the Ultimate High Ground: Next Steps in the Military Uses of Space*, (Santa Monica, CA: RAND Report, 2003), 29.
[42] Lambeth, *Mastering the Ultimate High Ground*, 24.

on an accelerated course for delivering more to the warfighter. Additionally, the sudden absence of a near-term threat in space allowed US forces to develop, acquire, and employ new space capabilities in a permissive environment. Traditional notions of space warfare and space control, cornerstones of US nuclear deterrence, soon dissipated as national security priorities shifted to regional, dynamic, and low-intensity conflicts.

Operation Desert Storm embodied the culmination of joint strategy, doctrine, and technological prowess that developed in the aftermath of Vietnam. Energized in part by strategic concepts derived by Warden and Deptula and built from earlier advancements in land power strategy, the US military was primed for mobilized and net-centric warfare. However, even military planners did not fully anticipate the level of success achieved against the Iraqi army. The onslaught of multiple attack vectors over air, land, and sea concentrated incredible firepower at specific points, and the notion of precision engagement achieved new status. The capacity to conduct cross-domain operations existed as a result of exquisite intelligence, global communications, rapid coordination, and deliberate firepower at the output. Ultimately, Desert Storm's success brought about sweeping vindication to the military's refined approach to warfare.

Space capabilities, designed and optimized for nuclear conflict, had enabled the unparalleled fusion of conventional forces on the battlefield and altered prospects on the conduct of war. Moreover, the ability to conduct precision strikes through the air limited requirements for land operations and drastically reduced friendly casualties. Technical advancements in electro-optical and multi-spectral reconnaissance capabilities produced unprecedented granularity in overhead intelligence gathering, and sophisticated SATCOM constellations delivered more communication pathways than ever before (although post-war analyses indicated that bandwidth was severely lacking). The most advertised space-based capability was the newly implemented Global Positioning System (GPS), enabling exact targeting and limited collateral damage through integration with precision-guided munitions (PGM). William Burrows provides a concise description of the instrumental role space played in the campaign's success:

> Iraqi forces were in effect blinded, decapitated, and obliterated by orbiting spacecraft as much as by bombs . . . and Tomahawk cruise missiles. Reconnaissance satellites located targets, including the overrated Republican Guard, exposing them to punishing aerial bombardment and

> then to General Norman Schwarzkopf's renowned flanking action, or left hook. Other satellites eavesdropped on signals transmitted by the Iraqis. Still others provided continuously updated data on the weather; instantaneously relayed communication between field commanders and their headquarters and between headquarters and the national command authority in Washington; guided both cruise missiles and manned aircraft to their targets; and, from way out at geosynchronous, tracked the Scud ballistic missiles launched at Israel and Saudi Arabia and sent warnings to those countries almost instantly.[43]

The new paradigm of conventional war changed expectations across the political, military, and public communities. As a result, after the war, the US military vigorously sought ways to expand its ability for net-centric warfare and fervently acknowledged the importance of securing access to space capabilities.

The end of the Cold War was perhaps even more significant as it opened the door for pursuing force enhancement capabilities without the pressure of balancing a near-peer competitor. Not only could the US military acquire highly sophisticated technologies for space, it could do so in a permissive environment. This new geopolitical context manifested itself through several trade-offs between traditional design philosophies and warfighter needs. For example, conventional force requirements in Desert Storm revealed a greater need for communication bandwidth than a nuclear-oriented architecture could support. The Milstar constellation (comprised of sophisticated, monolithic satellites, each the size of a greyhound bus) entered service just after Desert Storm but was designed to provide secure, survivable, and assured communications in the event of nuclear war—a true artifact of the Industrial Age. Its prioritized mission was autonomous, robust communications that could function in nuclear environments. The downside was its data rate—far too low to sustain conventional forces in a non-nuclear scenario. As a result, a second block of Milstar satellites was later produced to offer greater bandwidth for both strategic and tactical communications while continuing the requirement for communications that could penetrate nuclear fallout.[44] A similar trend

43 Burrows, 612.
44 United States Air Force Space Command, "Milstar Fact Sheet," http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5328 (accessed 12 April 2015).

took place with other space assets after the war, and a shift in organizational priorities followed suit.

The combination of Desert Storm successes, recognition of space as a force multiplier, and a unipolar world formed a unique set of circumstances for military strategists to consider, particularly those in the USAF. On one hand, space capabilities proved essential for the US military's preferred style of warfare, elevating the importance of space control in the minds of senior leaders. On the other hand, the end of the Cold War left a gaping hole in the threat environment, relegating concerns of space warfare to theoretical discord. Furthermore, an immediate push to downsize the US military inadvertently elevated the criticality of space capabilities as force multipliers while simultaneously limiting budget allocations to counter what amounted to conceptual threats. Over time the strategic imperative for space control never found traction beyond the rhetoric it generated. The United States came to rely on space more than ever before, and no one had the ability to prevent it. Defense budgets, acquisition priorities, space architectures, organizational structures, doctrine, et cetera were eventually guided by a new (unwritten) paradigm that assumed superior technologies and capabilities provided the requisite level of space superiority—in essence, space superiority was now a de facto condition. In space, the threat was gone.

Post-Cold War and Reorganization

A series of institutional and organizational changes ensued in the US military and intelligence community after the Cold War. As suggested earlier, follow-on approaches to the US space infrastructure proved indicative of the broader defense mindset. From a warfighting standpoint, the focus on space control morphed into a battle for institutional control. From an intelligence standpoint, the emphasis turned to justifying its existence. Most importantly, the US government struggled to articulate a clear vision for space power in the twenty-first century, preventing cohesive transformation and promulgating a space framework that remains convoluted in purpose and disjointed in capability.

In Desert Storm's immediate aftermath, the USAF moved to secure budget allocations and take the lead on the invigorated mission area. Air Force General Donald Kutyna, then commander of USSPACECOM, remarked, "Unless we have a sound space-

control capability, we may find ourselves in a conflict with a nation with space forces while we have no means to prevent space-supported attacks on ourselves and our allies." General Charles Horner, who succeeded General Kutyna at USSPACECOM, echoed the concern that the United States could potentially lose valuable lives in future conflicts "because we were unable to deny the enemy space-based intelligence and imagery."[45] In response, the USAF established the Space Warfare Center (SWC) in 1994, a direct reporting unit to AFSPC designed to "support combat operations through control and exploitation of space."[46] Comprised of a wide assortment of agencies, the SWC provided a formal venue for innovation and direct warfighter support while giving the USAF a foothold on the space enterprise.

Institutionally, the USAF reevaluated the applicability of the aerospace construct. Conventional wisdom aligned air and space mediums under one vertical continuum, and it influenced the relationship and priority given to operations—illustrated by the almost obsessive recognition of space after Desert Storm. The USAF—indeed, the entire defense apparatus—sought to redefine its identity in the post-Cold War world and began its transformative endeavor by articulating a new *Global Engagement* vision in 1996. The new projection of air power doctrine delineated the USAF into an "air and space force," with a particular emphasis on space as the wave of the future. Critics, including General Horner in 1997 (then retired), pontificated that the USAF was simply posturing itself for budgetary reasons and that the organization was not primed to orchestrate space endeavors on behalf of the joint force.[47] In reality, the United States as a whole was not unified in its vision—or capacity—to control or exploit space.

While the military struggled to establish a claim on space, the intelligence community also faced institutional challenges in the post-Cold War period. As capitalism permeated the geopolitical landscape, the Clinton Administration attempted to rejuvenate the flailing aerospace industry and compete with the other dominant spacefaring nations on an economic level. To this end, on February 24, 1995, President Clinton authorized the release of 800,000 previously classified pictures taken by the *Corona* reconnaissance program from 1960 to 1972. The US government had already

---

[45] Burrows, 611-612.
[46] Burrows, 611.
[47] Lambeth, *Mastering the Ultimate High Ground,* 1-2.

acknowledged the existence of the clandestine National Reconnaissance Office (NRO) in 1992, and the latest revelation provided substance on the true nature of US space capabilities. Contrary to predictions, the CIA was not completely averse to unveiling its mission in space and instead believed the demonstration helped justify its continued relevance in light of the Soviet Union's demise. To the rest of the world, sophisticated space capabilities were now accessible in a globalized market economy. Ultimately, the initiative worked as the first commercial reconnaissance satellite, *Earlybird I*, was built by a Colorado company and launched on a commercial rocket on December 24, 1997, out of Svobodny, Russia.[48]

The confluence of military posturing, intelligence agency validation, and an open-ended geopolitical environment created a precarious situation for national security. To the military, space control remained a mantra for acquiring authority, roles, and responsibilities and was not necessarily derived from a pressing strategic necessity. The US intelligence community now faced the potential for parity in space reconnaissance with commercial vendors, and no existential threat existed. Additionally, America's preferred way of war—that of limited, precision engagement—allowed it to develop new and disparate techniques in a relatively benign threat environment. The lack of direction and oversight in space soon became apparent, prompting congress to call for a Space Commission to investigate the Air Force's performance as custodian of military space and assess the defense establishment's capacity for securing space access in the twenty-first century. The 2001 Space Commission report concluded that the current space cadre (consisting of military, civilian, and commercial personnel with varying levels of expertise) was not developed appropriately and that the budgetary process limited the proper allocation of resources to the mission area. Furthermore, the report cited a deep concern for the growing prospect of a "space Pearl Harbor," or a surprise attack on critical—and increasingly vulnerable—space systems.[49]

After the 2001 report, a series of significant events and decisions transpired, all of which shaped the current space operations mindset. On September 11, 2001, the intelligence community received a violent jolt as it failed to recognize and warn of

[48] Burrows, 613-614.
[49] Lambeth, *Mastering the Ultimate High Ground*, vii.

impending terrorist attacks. Its overall infrastructure, however, was designed to collect information against state adversaries (primarily for nuclear deterrence), not to acquire tactical intelligence on indigenous terrorist groups.[50] The following years saw substantial transformation in the intelligence apparatus, as multiple agencies were brought under a unified structure headed by the Director of National Intelligence (DNI) to orchestrate national collection endeavors and assessments. From a space perspective, the space-oriented intelligence agencies (e.g., the CIA and NRO) retained authority for their space operations.

Militarily, earlier cries for space control capabilities shifted once again to a demand for more force enhancement, and controlling space fell to a suite of niche (but highly effective) capabilities to augment limited conflicts against technically inferior opponents. Moreover, in 2002, USSPACECOM—the warfighting organization originally configured to achieve space control—was deactivated after "it had become clear that neither the U.S. nor any other government had the money to do much in space" in terms of space warfare.[51] United States Space Command was rolled under USSTRATCOM, the successor to SAC, yet another organization vying for relevance.[52] Similarly, the SWC was rechristened the Space Innovation and Development Center (SIDC) as all warfare centers merged under a single entity at Nellis Air Force Base, Nevada, signaling an institutional detachment from the notion of space warfare. In 2006, the combatant command activated its Joint Functional Component Command for Space (JFCC SPACE), consolidating USSPACECOM assets and missions—albeit with a very limited concept and imperative for space control—under the new entity. The following year, JFCC SPACE activated the Joint Space Operations Center (JSpOC), established using the Air Force's approved and funded AOC model.[53] The JSpOC, in direct support of USSTRATCOM and geographical combatant commands, developed a capacity to orchestrate *military* space force enhancement capabilities in dynamic (and low-intensity)

---

[50] Taubman, 356.
[51] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It*, (New York, NY: Harper Collins, 2010), 35.
[52] Notably, the same year, USSTRATCOM assumed responsibility for joint cyber operations.
[53] As the executive agency for space, the Air Force component to JFCC SPACE—14th Air Force—provides forces to the warfighting agency through the 614th AOC.

environments while helping secure the nation's most sensitive information from space.[54] In the end, with the military and intelligence communities absorbed in combating global terrorism, the momentum for comprehensive space control objectives and capabilities faded.

A final analysis reveals that the shifting priorities and decisions for space operations exist due to the absence of any unifying space power vision or strategy. As recent as 2013, several space analysts expressed concern over the lack of direction in space. While visions and policies abound, the lack of consensus on a national space power strategy creates confusion in mission design, organizational structures, and operational priorities and in fact leaves the nation in a dire situation given its unavoidable dependence on space. As Eric Sterner notes, "The space program does not suffer from a lack of vision, per se, but the lack of an agreed set of filters through which one can prioritize resource allocation."[55] Further, Scott Pace noted key discrepancies between the 2010 National Space Policy (NSP) and the 2011 National Security Space Strategy (NSSS). Interestingly, the NSP verbiage refrains from pursuing international norms in space, while the NSSS articulates multilayered deterrence through the establishment of norms, revealing a startling confusion of authorities, roles, and responsibilities in the domain. Subsequently, at the Air Force level, Benjamin Lambeth expressed consternation over the service's lack of progress "toward developing and promulgating an agreed frame of reference for thinking systematically about the military potential of space."[56] Getting to the heart of the matter, Steven Lambakis, a senior national security analyst, concluded, "the United States is secure in space by default, not because there is a deliberate policy framework and well-resourced, organized, and strategically guided military force to guard national military space assets."[57] Indeed, the lack of strategic urgency has diverted attention from an impending issue that threatens to attack the US space infrastructure—and desired way of warfare—at the seams.

---

[54] CDR USSTRATCOM does not hold any authority over the intelligence community's space assets or operations. CDR USSTRATCOM and the DNI (or DNRO) coordinate mutual activities in the domain.
[55] Eric Sterner, ed., *America's Space Futures: Defining Goals for Space Exploration*, (The George C. Marshall Institute, 2013), 126.
[56] Lambeth, *Mastering the Ultimate High Ground*, 36.
[57] Steven Lambakis, *On the Edge of the Earth: The Future of American Space Power*, (Lexington, KY: The University Press of Kentucky, 2001), 1.

The Emergent Threat Environment

If nothing else, history shows that environmental change and human nature are constant. Both factors circumscribe war, and competition underlies provocations of conflict. As environments change, humans strive to gain control of their surroundings by leveraging advantages over their opponents. War offers a provocative glimpse into the core behavior of human nature and its fallible condition. For example, the advent of air combat occurred as a result of an inevitable duel between humans trying to gain and neutralize a technological (and *informational*) advantage. Likewise, in the twentieth century, the strategic environment shifted from a structured bipolar confrontation to an open-ended unipolar world fraught with ambiguous threats. From the US point of view, its newfound military dominance could offset the amorphous (yet manageable) risks that emerged around the world. From the international perspective, however, the US military was the only player left standing in the game, allowing adversaries to direct focus on probing for chinks in its armor. As human nature would have it, the US reliance on space provides an attractive target for adversaries to neutralize its asymmetric advantage. Space is a viable warfighting domain for those seeking to undermine US military superiority.

The strategic landscape is once again shifting. The international cooperation and commercial competition in space that ensued after the Cold War expanded the number of spacefaring nations from a small handful to a significant portion of the total. Nearly 60 nations and/or government consortia have routine access to space today, as well as several more commercial and academic organizations.[58] At the same time, China's perpetual rise as a budding world power extends to its aggressive strategy for establishing itself as a leading space power. Notably, the US space infrastructure was initially designed to function in an environment with only a limited number of participants, and only one true competitor in a strict bipolar arrangement. The new environment poses potentially serious risks to US national security as a wider variety of objects and owners exploit the domain's inherent advantages.

[58] US Department of Defense, *National Security Space Strategy* (Washington, DC: Office of the Secretary of Defense, 2011), 2.

While continuing its mission to combat terrorism, the US government has recently acknowledged the expanding field of participants in space and its implications on national security. The 2011 NSSS opens accordingly, "As more nations and non-state actors recognize [the benefits of space] and seek their own space or counterspace capabilities, we are faced with new opportunities and new challenges in the space domain. The current and future strategic environment is driven by three trends—space is becoming increasingly *congested*, *contested*, and *competitive*."[59] Certainly, the mere fact that the domain is increasingly congested gives rise to its contestation and competition. Similarly, in one of its final documents, US Joint Forces Command (JFCOM) offered a solemn assessment of the situation in 2010 by highlighting "the need to protect and operate our space systems in an increasingly contested and congested orbital environment. The relative vulnerability of space assets plus our heavy reliance on them could provide an attractive target for a potential adversary."[60]

Arms control activists and others who advocate for the natural sanctity of space dismiss such notions as alarmist or provocative. In particular, they cite multiple European, Russian, and Chinese attempts to ban weapons in space.[61] Furthermore, sanctuary supporters are quick to indicate that only the United States and Israel are reluctant to accept the proposals, implying that US policy decisions prevent the advancement of international desires.[62] However, a closer look reveals that Russian and Chinese diplomatic actions may in fact serve as a means for balancing US strength in the domain. Just as the Soviet Union sought to undermine US advantages through international protest, the current regimes engage diplomatically to limit US supremacy, regardless of any benevolence displayed. Moreover, a growing number of states are actively acquiring *and employing* counterspace capabilities *as they vocalize a need to ban*

---

[59] US Department of Defense, *National Security Space Strategy* (Washington, DC: Office of the Secretary of Defense, 2011), 1.
[60] United States Joint Forces Command, *The Joint Operating Environment 2010* (Suffolk, VA: Joint Futures Group, 2010), 37.
[61] Moltz, 31. Of note, China began its public call for banning space weapons in 2002 in Geneva, three years after the American arms control community first formally lobbied for de-weaponizing space. See Michael Pillsbury, *An Assessment of China's Anti-Satellite and Space Warfare Programs, Policies, and Doctrines*, Report to U.S. – China Economic and Security Review Commission, 19 January 2007, 5.
[62] Moore, xviii.

them, effectively tying the hands of US strategists through the pursuit of international norms with which they may not intend to comply.

Undoubtedly, counterspace activity is a growing trend. Russia displays a rich history of counterspace expertise from the Soviet Union, while Iranian and North Korean activities disclose increasingly sophisticated counterspace arsenals. In the midst of increased counterspace activity around the globe, China currently boasts the most aggressive and deliberate program. In March 2014, Douglas L. Loverro, deputy assistant secretary of defense for space policy, testified before congress that countries "have recognized that if they are to challenge the United States, they must challenge us in space . . . and they are endeavoring to do so."[63] While still seeking to promote and preserve the peaceful use of space, the United States cannot afford to assume all spacefaring nations intend to uphold the domain's sanctity, particularly in a time of war. A brief synopsis of recent Chinese counterspace endeavors and the strategy that drives them—aimed at inhibiting US strategic interests on earth—reveals why.

China and Information Dominance

China presents a unique and impending challenge for US strategists. The country's invariable rise as a world power naturally creates concern in the US government, particularly as the international system slowly rebalances itself in the vacuum left by the Soviet Union's collapse. From a national defense perspective, China's strategic transformation over the past two decades involves a deliberate and systematic approach for neutralizing US preponderance, specifically in the Pacific region. As discussed in Chapter 2, China closely observed US activity in Desert Storm and subsequently revamped its approach to warfare. Instead of fielding massive armies to deliver overwhelming force, China pivoted toward more discrete, asymmetric warfare in the unified pursuit of *information dominance*.

The People's Liberation Army (PLA) conducted a series of investigations after Desert Storm that formulated its new outlook, specifically on the concepts of cyber and space warfare. In 1995, the PLA concluded that local wars under high-tech conditions

[63] Sergeant First Class Tyrone C. Marshall, Jr., "Officials Update Congress on Military Space Policy, Challenges," American Forces Press Service, 12 March 2014, http://www.defense.gov/news/newsarticle.aspx?id=121826 (accessed 12 April 2015).

were more likely and that the approach to such wars "would place much greater emphasis on joint operations."[64] According to Chinese estimates, the United States employed 70 satellites during Desert Storm, collectively providing 90 percent of its strategic intelligence and 70 percent of transmitted data. As Forrest Morgan observed in his RAND report years later, "The enemy's benefit in attacking space assets is proportionate to the United States' dependence on the capabilities they provide."[65] Not surprisingly, then, controlling and denying access to space took center stage in the PLA's revamped strategy.[66] By 2004, the Chinese government modified its assessment of modern warfare as localized and "informationized." In this instance, *informationized* referred to a broader concept of information warfare, somewhat similar in design to the information environment. Dean Cheng provides a good summary of the Chinese-derived term:

> *Informationized conditions*, in this context, did not simply refer to computers and cyber warfare. Rather, the informationized battlefield . . . is one in which all the relevant military activities—including tactics and operations as well as decision making—are digitized, and military materials and equipment are managed through advanced information technology. The shift in terminology reflected the PLA's conclusion that, among the various high technologies, the most important with the most far-reaching impacts are those relating to information management.[67]

Two years later, in 2006, the PLA refined its notion of warfare once again to the importance of precision strikes to control conflict and disrupt the enemy's decision-making potential. Underscoring the PLA's intent for precision engagement and control was the attainment of information superiority. As expected, the PLA, now formally charged with controlling space, viewed military space operations as essential to acquiring information dominance. Indeed, PLA leadership believed that "establishing space dominance, establishing information dominance, and establishing air dominance in a conflict will have influential effects."[68]

Prior to 2006, the Chinese government authorized the release of several unclassified papers outlining various approaches to space warfare. Colonel Li, a

---

[64] Dean Cheng, "China's Military Role in Space," *Strategic Studies Quarterly*, Spring 2012, 58.
[65] Forrest E. Morgan, *Deterrence and First-Strike Stability in Space: A Preliminary Assessment*, (Santa Monica, CA: RAND Report, 2010), xiii.
[66] Cheng, 59.
[67] Cheng, 61.
[68] Cheng, 62.

professor at the PLA's defense university, penned a five-step plan for producing a space warfighting infrastructure in 2001. The document advocated for the establishment of *covert* capabilities that could circumvent international regulations. Li also promoted China's now prevalent concept of the "assassins mace," an asymmetrical approach to warfare against a superior opponent.[69] Subsequent documents in 2002 and 2005 expanded on Colonel Li's concepts and called for additional counterspace capabilities, including the construction of space-based strike platforms, mobile ASATs launched from ships and submarines, laser weapons, and multi-layered electronic warfare. Additionally, the documents listed specific US space systems as key targets of engagement.[70]

As if on cue, 2006 marked a tangible turning point in the security environment. Until then, literature remained China's dominant form of posturing in space. While the PLA had undergone significant transformation as an institution, it had not displayed a significant capability to challenge US access in the domain. However, a series of surprising activities occurred in the space domain over the next several years. In 2006, only a few years after China's initial report on information dominance, the Director of the NRO confirmed the Chinese had targeted a US satellite with a ground-based laser.[71] The following year, in 2007, China conducted its first direct ascent ASAT (DA-ASAT) test—a missile strike against one of its obsolete weather satellites. Most importantly, *the Chinese DA-ASAT test ended a decades long moratorium on ASAT tests observed between the United States and Soviet Union*.[72] An operational success (but an international faux pas), the DA-ASAT obliterated the satellite, sending thousands of pieces of space debris into orbit. The years following 2007 brought additional tests of more sophisticated counterspace technologies and operations. Critically, the events suggest that China initiated a deliberate procurement strategy for capabilities to fulfill its previously theoretical objectives. As seen through the legacy of Sun Tzu, the Chinese culture values deception, but it is difficult to discount the momentum generated by strategic modifications, organizational changes, and budgetary decisions that coincide with the approach.

---

[69] Pillsbury, 22-23.
[70] For further analysis, refer to Pillsbury, 7-20.
[71] Pillsbury, 3.
[72] Lt Col Anthony J. Mastalir, *The US Response to China's ASAT Test*, (Maxwell AFB, AL: Air University Press, 2009), vii.

The emergence of China as a world and space power alters the strategic calculus for US national security, regardless of its intentions. Since the end of the Cold War, the US government and military had the "luxury" of time and technical superiority to dictate actions in the domain with minimal effort and even less resistance. As the second full decade of the twenty-first century reaches its halfway point, the window of opportunity for the United States to develop and implement a unifying strategy for space on its own terms is almost gone. Furthermore, assumptions on the capacity to take certain actions in war are no longer valid, and yet the US military has constructed and financed a method of war that flows from those terms. As Dean Cheng accurately surmised, "Unlike previous conflicts in the Middle East, the Balkans, and Central Asia, if the United States engages in a conflict in the western Pacific, it will be confronted by a nation with a comprehensive set of space capabilities to counter America's own."[73]

Conclusion

The US space culture embodies more than just space operations. Its infrastructure provides a window into the philosophies that shaped national defense priorities in the second half of the twentieth century and even the first two decades of the twenty-first. As the joint force transitions toward Information Age warfare, it must understand the strategic, operational, and tactical realities of the institutions and organizations that comprise it. Indeed, Gareth Morgan's keen perspective on organizational transformation holds true—one must appreciate the basis of current paradigms before instigating change. Analysis in Chapter 3 revealed an outmoded mentality of space operations in the new context of Information Age warfare, a critical shortfall in a framework that places space as a cornerstone of information control. In this regard, the US space program's history offers insight into the geopolitical and operational considerations that formed the space community's culture and its perceived role in national defense. Moreover, the complications of the space infrastructure's strengths and weaknesses belong to the *entire* joint force rather than just the space community.

After reviewing key events and considerations in the history of US space operations, several points converge to paint a picture of the current culture. First, the US

[73] Cheng, 55.

space infrastructure formed under the oppressive weight of the Cold War and was thus constricted by geopolitical imperatives. National prestige, power, and security were all at stake as the United States battled the Soviet Union for preeminence, and the space domain offered a new venue for competition. Furthermore, to prevent each other from gaining any notable advantage in space, both sides ratified treaties that limited aggressive space-based activities and nullified any incentives for independent action. In essence, space became a highly politicized and controversial domain from the onset.

Second, to detect a surprise nuclear attack without provoking war, decision makers turned to space-based reconnaissance as an attractive option. In so doing, US space operations were prioritized by strategic intelligence collection requirements, and the initial cadre of space professionals were pooled from the scientific and engineering communities. Consequently, information gathering was focused on intelligence *from* space rather than *for* space, and early space operators did not inherit a military mindset for controlling the domain.

Third, and relatedly, the US military's involvement in space grew under the auspices outlined above. Although great strides were made in developing a robust assortment of space capabilities—indeed, an intricate system of *information collection and dissemination networks*—the capacity to assure domain access was tempered by a myriad of policy regulations. Additionally, military space operations commenced apart from ongoing, highly secretive intelligence operations. The nuance is significant, although not fully appreciated. While the military sought innovative ways to gain space control, it lacked the institutional framework to acquire the exquisite intelligence needed to fulfill the concepts it explored. Again, the warfighting community—including space—remained focused on what space capabilities delivered (i.e., strategic intelligence and force enhancement) and less on the information requirements necessary to control the domain. This was due in large part to the long-standing acceptance of the *aerospace* foundation set by General White in 1958—a mindset that continues to influence perceptions of air, space, and even cyberspace.[74] Space was merely a continuation of air, and space superiority was a derivation of air superiority.

---

[74] The correlation between air and space domains is deeply ingrained in service tradition, accounting for the current delineation between space and cyberspace that overlooks their functional relationship.

Fourth, the experiences of Desert Storm along with the end of the Cold War created an opportunity for space operations to surge into the forefront. With the existential threat gone, the US could pursue its new way of warfare with minimal opposition. Thus, space force enhancement capabilities soared, as did the demand signal for their services, while the impetus for space control subtly diminished. At the same time, the new global economy proliferated previously restricted technologies, giving rise to commercial access and international participation. Despite the growing number of objects and operators in space, the events of 9/11 once again redirected US military attention. Space capabilities persisted as force multipliers, and intelligence services exploited space-based intelligence and other sources for dissecting low-tech terrorist networks. Intelligence from space continued to trump intelligence for space, perhaps even more drastically in the post-Cold War environment. Despite verbiage to the contrary, space capabilities were essentially taken for granted as no one could prevent the United States from accessing them.

Underscoring the entire story is the lack of consensus on a long-term, unifying strategy for US space power. The dichotomy between military and intelligence operations in space, a restricting view of aerospace as a physical continuum, institutional posturing for budgetary allocations, and massive organizational changes that diminished the military's ability to control access to the domain all occurred as a result of shifting priorities that catered to the immediacy of geopolitical environments. Consequently, the US space infrastructure is a heterogeneous mixture of technologies, expertise, priorities, perspectives, and structures that are realistically designed to provide space-based services in a largely permissive environment. Overall, the joint force is equally varied in its expectations of space and is therefore unprepared for securing access to the domain in future conflicts.[75]

The evolving strategic landscape once again presents a unique challenge to national security. Forrest Morgan provides an excellent synopsis of the transition that occurred in space after Desert Storm and the Cold War. In essence, the subtle decoupling of space capabilities from nuclear warfare created a level of instability in space

[75] Today, space is the only domain supporting US military operations that joint forces do not actively seek to control—including cyberspace.

deterrence—*space support became a cornerstone of conventional warfare while still remaining fixed in the nuclear deterrence architecture*, making it a valid *and vulnerable* target for potential adversaries.[76] As the United States engaged in localized, low-intensity conflicts that thrived on globally networked communications, other nations observed, learned, and produced their own indigenous space and counterspace capabilities. Russia maintains operational expertise, but China has shown a systematic and deliberate approach to gaining control of the environment through information dominance. China continues to demonstrate its intention for challenging US dominance in space, both diplomatically and militarily. In an emergent threat environment, the United States may find itself flatfooted and unable to assess, respond to, or even recognize attacks in the domain.

The criticality of information control in the twenty-first century elevates the strategic urgency of the situation—the loss of which could prove catastrophic for national security. By adopting a comprehensive information control strategy, the United States can simultaneously posture its joint force and its space infrastructure to forge a unified and potent approach to warfare. Thus, *the United States should adopt a space control strategy that binds its activities in the pursuit of information control*.

Given this historical background and the emerging threat environment, new questions arise as to the efficacy of the current space posture. Specifically, how does a military know that it holds space control or superiority? How does it know when space control or superiority is lost? What actions are required to achieve control and/or superiority in space? What agency is responsible for obtaining and assessing space control? And finally, what is the proper role of the military in space? The final chapter opens the door to this discussion and provides areas for consideration when formulating a space control strategy within the overarching premise of information control.

---

76 Morgan, 24.

Chapter 5

Space Control—A Cornerstone of Information Control

This favoritism [toward pursuit aircraft] produced a rapid growth of this flying specialty; but at the same time it obscured the problem of national defense and prevented a correct understanding of what the command of the air consists in.

- Giulio Douhet

Figuring out how to use space systems to put information into the cockpit in order to more accurately drop bombs from aircraft…. This is not space warfare; it is using space to support air warfare.

- Senator Bob Smith

The weapon of superior reach or range should be looked upon as the fulcrum of combined tactics.

- J.F.C. Fuller

The primary consideration for any tactician is the threat. What are the enemy's capabilities?

- C.R. Anderegg

The analysis now turns to examine what a notional space control regime *could* look like within an overarching information control strategy aimed at preserving the US military's ability to operate as desired. The chapter begins with an overview of the military's role in space, addressing the final question posed in Chapter 4. The remaining sections of the chapter build a framework for examining the more penetrating inquiries regarding space control and space superiority. To this end, the definitions of information control and information superiority provide context for theoretical constructs of space control and space superiority, respectively. The study continues with a broad overview of the space domain—its basic architecture, advantages for information collection and dissemination, and established missions—and subsequently outlines a space control methodology. With the historical setting presented in Chapter 4 as a background, the analysis concludes by evaluating the military's capacity to achieve space control as described. Specifically, the evaluation assesses extant US military space control doctrine, organization, training, materiel, leadership, and facilities (DOTMLPF) as well as its supporting intelligence apparatus.

The final section provides insight into the larger considerations associated with transforming an Industrial Age military into a force capable of securing national interests in the Information Age. Importantly, the concepts of space control presented here align

with *military* and *intelligence* space operations and do not directly incorporate aspects from a whole-of-government perspective. However, the proposed construct does set the foundation for further integration with other government, civil, and commercial entities. In effect, military requirements for space control involve activity across the entire spectrum of conflict—during peacetime and war—thereby adhering with the military's overall responsibility of constant preparedness, vigilance, and maximum effort.

As a final note, layering a space control strategy within an information control framework may appear to confine the role of space in national security. However, in the twenty-first century, information control is paramount, and is in fact the foundation for all other activity in the domain. Any further exploitation of space cannot successfully occur without first securing information control—that is, control of infospheres based on a national or military strategy's information requirements. Thus, space control and space superiority are subsets of information control and information superiority, respectively, and establish requisite conditions for supplementary domain activities, as required. Pragmatically, the proposed space control concepts of operation are universal in purpose and extend beyond initial attainment of information-centric objectives. The window of opportunity for determining the appropriate direction in space is shrinking rapidly, and the US military can no longer assume that historical precedents will ensure its freedom of action in the domain.

The Role of the Military . . . in Space

National security incorporates a collection of capabilities designed to project and employ sources of power. Among these capabilities is the authority of the state to threaten and impose sanctioned violence against another state in the pursuit of national objectives. The US military is uniquely suited and designed to accomplish this *specific* function. The military's primary purpose is to "be prepared, and when called upon by the legitimate governing authority, to maximize violence within the constraints placed upon it."[1] To orchestrate such an undertaking, the military divides its operations and organizational responsibilities by domains, as examined in Chapter 3. In fulfillment of

[1] Dr. Everett C. Dolman, "Astropolitik: A Case for Weapons in Space" (lecture, School of Advanced Air and Space Studies, Maxwell AFB, AL, 16 March 2015).

political and military objectives, military forces seek to control or contest access to each domain, as required. Collectively, the control of individual domains contributes to the overall strategic advantage of full-spectrum superiority, setting optimal conditions for the maneuvering and exploitation of other national security measures. The capacity to coordinate and conduct cross-domain operations for the attainment of full-spectrum superiority anywhere in the world is made possible through the collection and dissemination of global, near instantaneous, and accessible information—key attributes of space and cyberspace networks.

In this regard, because militaries increasingly rely on space-based capabilities to project and employ force, warfare in and through the space domain is unavoidable—*the essence of strategy dictates it*. Thus, outlawing space warfare does not necessarily preserve the sanctity of space, as it simply establishes an artificial barrier viable primarily in peacetime. Such initiatives inhibit the US military from preserving its ability to act in a hostile environment and, ultimately, from fulfilling its essential purpose.[2] A space control strategy, predicated on the possibility of space warfare, exists to ensure space-based capabilities are available to decision-makers, warfighters, and even the civilian populace throughout the spectrum of conflict.

Toward A Space Control Strategy and Concept of Operations

Space control is a vital component for achieving information control in modern warfare. To construct a practical model for space control, a brief review of information control and information superiority theory is necessary. Subsequently, an examination of the basic space architecture provides operational context for building a space control concept of operations within a space and information control strategy. Of note, space control and information control are prerequisites for more aggressive superiority strategies and therefore receive greater attention in this analysis.

[2] For instance, Russia and China openly advocate for banning space weapons while continuing to enhance their own asymmetrical advantages. The United States currently holds a distinct—yet diminishing—advantage in the domain, and the two countries are strategically postured to deny its ability to preserve it.

Information Control and Information Superiority Revisited

Recall the operational and strategic definitions of information control and information superiority presented in Chapter 3. As stated, the Information Age is characterized by global, near-instantaneous, and accessible information and therefore promotes a certain level of parity between traditionally strong and weak actors. As a result, concepts of information control and superiority assume slightly different implications than customary designations of the terms. Table 2 summarizes the revised concepts accordingly.

Table 2: Operational and Strategic Definitions of Information Control and Superiority

	Operational	**Strategic**
Information Control	Freedom of access, maneuverability, and exploitation of established infospheres—commensurate with one's strategy—and the ability to prevent others from denying that freedom. *Control of the infosphere begins with controlling access to the physical dimension, or the information collection and dissemination systems employed*.	The ability to recognize and prevent degradation of infospheres that would lead to an undesirable retrograde in a particular strategy or way of warfare.
Information Superiority	A relative condition of control—one side is able to control infosphere access as needed, while the opponent is unable to exert the level of control required by his strategy.	The ability to maintain information control—relative to a strategy's needs—while eliminating the adversary's ability to recognize and prevent degradation of his own infospheres relative to his strategy's needs.

Source: Author's Original Work

By inference, information control is inherently defense-oriented, while information superiority emphasizes an offensive approach.

Information control begins with identifying and securing access to the infospheres that support a particular strategy, campaign, operation, and/or mission. While an infosphere's information dimension contains vital messages for interpretation, decision-making, and action, the infosphere's physical dimension establishes its structure and therefore serves as the focal point for implementing basic control measures. As explained, the physical dimension is comprised of networked information systems

employed to collect and dissemination requisite information. At its core, space and cyberspace systems collectively comprise the backbone of an infosphere's physical dimension by enabling global, near-instantaneous, and accessible communications.

Theoretical Concepts of Space Control and Space Superiority

In this theoretical model, concepts of space control and space superiority develop in relation to the information control strategy that drives them. Space control therefore involves freedom of access, maneuver, and exploitation of the space domain, as required, and the ability to prevent others from denying that freedom. Furthermore, space superiority is a relative condition of space control, as one side is able to control access to the domain as needed, while the opponent is unable to exert the level of control required by strategy, primarily due to intentional degradation or denial of access. In this regard, if an opponent's strategy does not require extensive use of space-based capabilities, then simply having a greater presence or technical advantage in the domain does not necessarily constitute space superiority in relation to the larger context of information control or information superiority. In other words, information control and information superiority involve the combined protection or denial of integrated information collection and dissemination systems that comprise an infosphere's physical dimension. Therefore, *an information control or information superiority strategy (or campaign) dictates the respective level of control or superiority needed in space and cyberspace*. Space control is not the ultimate goal.

The Space Architecture

An overview of the basic space architecture, information collection and dissemination opportunities, and doctrinal mission sets provides a transition for developing and assessing a practical concept for space control. The basic space architecture remains unchanged since the dawn of the space age. Regardless of their ultimate configuration, all space architectures consist of three segments: a terrestrial node, the orbital asset, and the portion of the EMS that connects them (i.e., communication links). In essence, the terrestrial and orbital segments play host to the physical components that comprise an infosphere's physical dimension, whereas the

EMS segment embodies an infosphere's information dimension. Figure 9 illustrates the three segments of the space architecture.

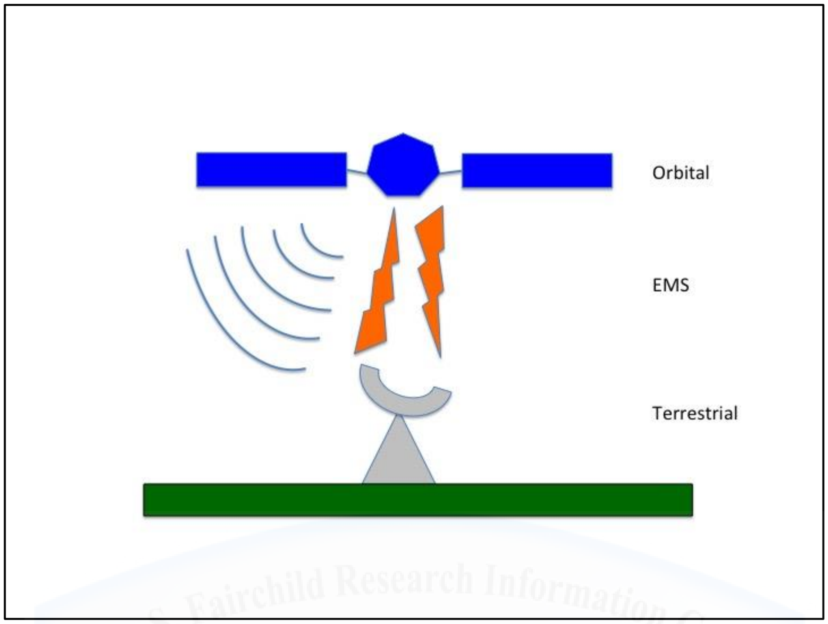

Figure 9: Three Segments of the Space Architecture
Source: Author's Original Work

The terrestrial segment involves a wide range of systems and users designed to control or exploit space assets and capabilities. Assets in the terrestrial segment include globally dispersed satellite C2 nodes (e.g., the Air Force Satellite Control Network, or AFSCN); space surveillance radars (e.g., ground-based assets in the SSN); launch sites; relay stations; and users (e.g., national and theater command centers, commercial and civil facilities [power grids, commerce hubs, and transportation centers], weapon systems, civilians, and warfighters). From a military perspective, the orbital segment presently incorporates *contiguous space*, or the region of outer space between earth's atmosphere and the moon.[3] For the purposes of this analysis, outer space begins at approximately 130 kilometers altitude, or the altitude at which an object will make at least one complete rotation (orbit) around the earth before reentering the atmosphere. The orbital segment includes man-made satellites and the orbits through which they currently *or potentially* traverse.

[3] Donald Cox and Michael Stoiko, *Spacepower: What it Means to You*, (Philadelphia, PA: The John C. Winston Company, 1958), xvi.

Finally, the EMS involves regions of the spectrum employed to collect and disseminate data (e.g., radio frequency, visible, infrared, etc.), including directed energy. As explained in previous chapters, the EMS provides communication pathways between ground-to-orbit (e.g., satellite C2, communication uplinks, and space surveillance), orbit-to-ground (e.g., satellite telemetry and communication downlinks; data collection of terrestrial activity such as space-based imagery), and orbit-to-orbit (e.g., satellite crosslinks to circumvent earth's atmosphere while transmitting data around the globe). Notably, a fourth communication pathway, ground-to-ground, enhances the space architecture and constitutes an integration point with cyberspace. The EMS embodies information collection and dissemination properties across the entire space architecture, revealing the inherent function of space systems as information networks.

In reality, the space domain incorporates architectures that are inherently global in scale. The encompassing nature of space and the geographical distribution of terrestrial assets indicate that space capabilities supporting a specific JFC will rely on space architectures that span multiple combatant commands (CCMD). Figure 10 provides a modified example of the global space architecture—representative of an infosphere created specifically for space operations.

Information Collection and Dissemination and the Space Domain

The space architecture reveals fundamental aspects of information collection and dissemination unveiled in Chapter 1. First, the space domain (or medium) offers unique advantages and opportunities for information collection, which entails access and method. In terms of *access,* outer space encompasses the entire earth (beginning at an altitude of 130 kilometers); therefore, objects in space hold an incredible vantage point for surveying activities in terra. Depending on altitude, coverage may range from a small swath of earth to nearly one-third of its surface. Another function of altitude, satellites have no physical obstacles (or political barriers such as state sovereignty) to contend with as they traverse across their natural orbits above the globe. Moreover, at a cost to propellant and lifespan, satellites have limited maneuverability to adjust their orbital planes in support of new collection requirements. Furthermore, satellites in orbit travel at speeds unattainable on earth. For example, objects in sustained low earth orbit (LEO)—

between approximately 250 to 1,500 kilometers altitude—attain speeds of 17,500 miles per hour.[4] At this rate, LEO satellites orbit the earth once every 90 minutes (termed the *orbital period*). From an information collection standpoint, satellites can access multiple locations on earth in brief periods of time.[5]

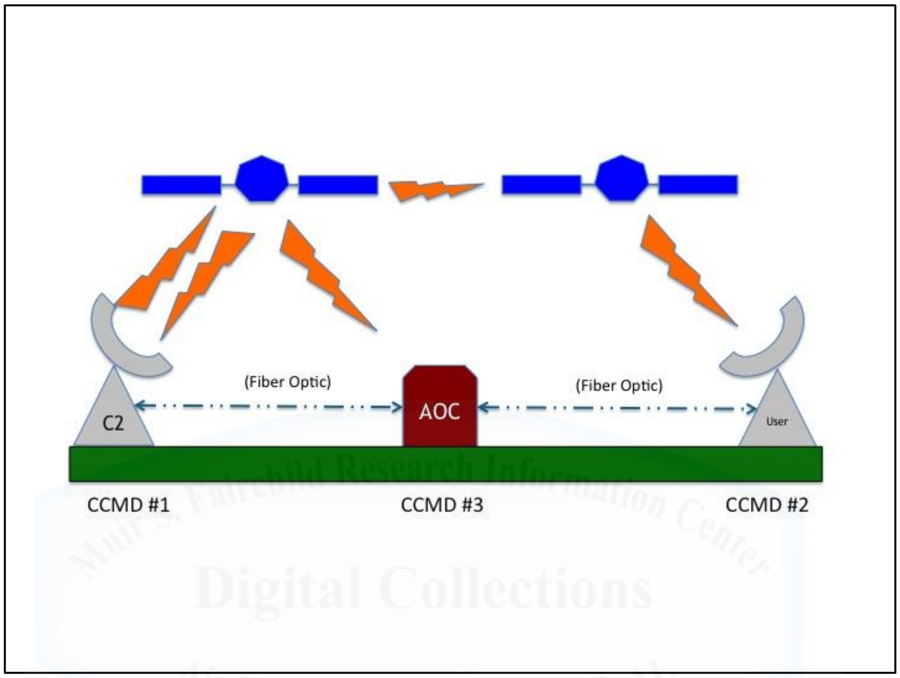

Figure 10: Notional Global Space Network
Source: Author's Original Work

In looking at *methods* used to collect information, space also provides unique opportunities to utilize various collection technologies. Space is a vacuum, which allows for less interference or natural manipulation of the EMS and, as a result, greater information integrity (evoking the "CIA Triad"). In contrast, earth's atmosphere distorts EMS wavelengths, requiring various technical solutions to compensate for signal loss

[4] Although outer space extends *ad infinitum*, satellites have limited agility once in orbit. Orbital speeds prevent rapid maneuvering and require inordinate amounts of propellant to adjust velocity vectors. In some cases, a satellite may not be able to access a new location on earth because of these orbital limitations, requiring access from another satellite, the employment of terrestrial-based assets (i.e., airborne ISR platforms), or, in extreme cases due to prohibitive cost and availability, insertion of a new satellite in the appropriate orbit. Therefore, while satellites remain in orbit for years and have the capacity to access multiple points on earth during that time, they are not as maneuverable as airborne collection assets.
[5] For persistent and global coverage, multiple satellites of the same type are typically placed into similar orbits. Predesigned collections of satellites are called *constellations*. Constellations incorporate *phasing*—optimized separation—of assets to ensure optimal collection of required areas.

(e.g., increased power output and forward error correction, or digitally adjusting the received signal based on expected input). Thus, sensors in orbit (onboard *payloads*) can collect information anywhere along the EMS—depending on a sensor's respective technology—with minimal degradation. Additionally, a satellite can host many payloads at once (an economical solution as much as it is operational), maximizing collection opportunities across a constellation.[6] Overall, the space domain provides an excellent medium for gaining access and exploiting a wide range of methods to collect information.

In addition to information collection, the space domain allows for rapid and global information dissemination. Information dissemination, characterized by speed and reach, thrives in the vacuum of space. Just as space allows for unfettered information collection through the EMS, the domain offers a relatively benign environment for digitized information dissemination. Because the EMS moves at the speed of light, space communications (like terrestrial communications using the EMS, including ground-based space surveillance) are inherently rapid. Likewise, orbital altitudes elevate data transmissions above terrestrial impediments such as mountains and trees—termed *obscura* in the space operations lexicon—allowing for natural, unobstructed signal propagation around the earth (typically enhanced through satellite crosslinking, or space-to-space communications, to exploit earth access from satellites in other orbital locations). Therefore, as illustrated, the space domain is ideal for global reach. In sum, the space domain is optimal for information collection and dissemination technologies, particularly those that are rapid, global, and accessible. Indeed, space-based capabilities are inherently informational, in large part due to the advantages afforded by the space medium.

Military Utility of Space—Current Mission Sets

Joint and service doctrines compartmentalize the above aspects of space operations into five mission sets. Codified space mission sets include space force enhancement (SFE), space situational awareness (SSA), space support, space force

[6] A satellite "bus" refers to the platform that hosts multiple health and status subsystems—it is the basic framework that supports payloads. The payload gives a satellite its operational capability (i.e., SATCOM, IR, PNT, EO). Each payload may support multiple users (national to tactical) simultaneously. Furthermore, each payload onboard a satellite may belong to different agencies, and the satellite bus operator may differ from the payload owner(s) and operator(s).

application, and space control. Table 3, derived from Joint Publication 3-14, describes each mission area below.

Table 3: Space Mission Areas

Mission Area	Description
Space Force Enhancement (SFE)	Increase joint force effectiveness by increasing the combat potential of that force, enhancing operational awareness, and providing critical joint force support. Composed of ISR; missile warning, environmental monitoring; SATCOM; and PNT.
Space Situational Awareness (SSA)	Involves characterizing space capabilities operating within the terrestrial environment and the space domain. SSA is dependent on integrating space surveillance, collection, and processing; environmental monitoring, processing and analysis; status of US and cooperative satellite systems; collection of US and multinational space readiness; and analysis of the space domain. It also incorporates the use of intelligence sources to provide insight into adversary use of space capabilities and their threats to our space capabilities while in turn contributing to the JFC's ability to understand adversary intent.
Space Support	Includes the essential capabilities, functions, activities, and tasks necessary to operate and sustain all elements of space forces throughout the range of military operations. Components of space support include: spacelift, satellite operations, and reconstitution of space forces.
Space Force Application	Combat operations in, through, and from space to influence the course and outcome of conflict by holding terrestrial targets at risk. Includes ballistic missile defense and force projection capabilities such as ICBMs.
Space Control	Supports freedom of action in space for friendly forces, and when necessary, defeats adversary efforts that interfere with or attack US or allied space systems and negates adversary space capabilities. It consists of offensive space control (OSC) and defensive space control (DSC).

Source: JP 3-14, Space Operations, 29 May 2013, x-xi.

In reviewing joint verbiage and intent, SSA underscores all other military space operations, while SFE represents the central purpose for operating in space. Although all mission areas form a synergetic relationship (physically through the formation of space-centric infospheres), SSA, space support, and space control *exist primarily to support and enable SFE capabilities*. Critics may argue that SSA enables all mission areas, and even supports diplomatic options, implying its preeminence in space operations. Nevertheless, the operational imperative for SSA is to ensure SFE capabilities are available for decision-makers and warfighters at all levels. Space support operations are intended to provide assured access to space through the terrestrial segment (e.g., terrestrial launch sites and satellite C2), while space force application, in its current context, connotes a peripheral mission that exploits the domain for rapid traversal of ground-to-ground or ground-to-air missile engagements. The space control mission area, the subject of the present study, is theoretically designed to secure access to the domain, as required, via a

combination of offensive and defensive measures. Conceptually, space control sets ideal conditions for all other mission areas and is a requisite for space superiority.

Strategically and politically, the space mission areas matured at different rates, and even experienced various levels of acceptance. For instance, as Benjamin Lambeth explained, the SFE and space support mission areas are “politically benign, with no sensitivities attached other than cost considerations.”[7] The same is true for the SSA mission. Space support experienced a significant upgrade in the form of the Evolved Expendable Launch Vehicle (EELV) program, an initiative currently contracted between a conglomerate of Boeing and Lockheed Martin (known as United Launch Alliance, or ULA) to provide the Department of Defense with reliable—albeit costly—launch services.[8] Similarly, SFE capabilities such as SATCOM, PNT, ISR, and missile warning received state-of-the-art additions to their constellations, providing the most technically advanced support to national endeavors. Space situational awareness incorporates a wide variety of capabilities, underscored by space surveillance operations developed over fifty years ago. Again, SSA enables decision making at all levels, and is therefore considered a priority for sustainment. Nevertheless, the emergent threat environment places exceptional strain on the aging surveillance architecture, a potential problem area for future space control operations. Although space support, SFE, and SSA capabilities are extremely expensive and require close scrutiny in an era of restricted budgets, “they do not entail higher level strategy and policy sensitivities,” indicating a general willingness to maintain or even increase funding.[9]

Conversely, space force application and space control tend to provoke political and public wrath and are seen as artifacts of a Cold War mentality. The history of space operations provides insight into the highly politicized arena of space warfare, effectively restraining the potential of space control. Indeed, “because [space force application and space control] envisage direct space combat functions, they have long been hobbled not just by cost considerations but also by a pronounced national ambivalence concerning

---

[7] Benjamin Lambeth, *Mastering the Ultimate High Ground: Next Steps in the Military Uses of Space*, (Santa Monica, CA: RAND Report, 2003), 97.
[8] Lambeth, *Mastering the Ultimate High Ground*, 97. Despite ULA’s reliability, the process for launch scheduling—above and beyond ULA—remains methodical and bureaucratic, restricting the ability for the Department of Defense to reconstitute its space-based capabilities rapidly, a point discussed in the next section.
[9] Lambeth, *Mastering the Ultimate High Ground*, 97.

space as an arena of warfare."[10] Additionally, arms control activists, a powerful lobby on the international stage, seek to prevent the weaponization of space, believing that the mere existence of potentially aggressive capabilities creates undue competition in the domain.[11] From this perspective, arms control activists initially sought to ban space-to-ground weapon systems, a specific aspect of space force application. In some cases, however, activists also seek to ban "any system whose use destroys or damages objects in or from space."[12]

A more holistic view of space operations and Information Age warfare reveals the danger of such an obstructive view of space control. Expanding on the overview of space architectures, domain advantages, and mission sets discussed above, the analysis now turns toward building a notional construct for space control in the broader context of information control. The new paradigm offers a counterpoint to the assumptions that traditionally hindered the advancement of military space operations and now threaten to inhibit US national defense options in the future.

A Space Control Methodology

To transition from theory to practice, the theoretical concept of space control now returns to the fore. A space control strategy ensures freedom of access, maneuverability, and exploitation in the space domain. Incorporating the practical design of space architectures into the theoretical model, *a modified space control concept of operations involves securing freedom of access, maneuverability, and exploitation of the terrestrial, orbital, and EMS segments for the ultimate purpose of preserving spaced-based information collection and dissemination capabilities*. Furthermore, space control involves the ability to prevent adversarial attempts at denying such freedom, emphasizing coordinated defensive operations—both active and passive—across all three segments.

Space control operations in each space segment are unique and must be integrated to achieve the overall objective. Space control operations in the terrestrial segment involve the identification and protection of ground-based assets. These assets include,

---

[10] Lambeth, *Mastering the Ultimate High Ground*, 98.
[11] This view falls in contrast to the discussions of human nature, control, and strategy outlined in Chapter 1.
[12] James Clay Moltz, *The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests*, (Stanford, CA: Stanford University Press, 2008), 43.

but are not limited to: launch sites and launch vehicles, satellite manufacturing facilities, satellite C2 centers, data relay stations, space surveillance assets, and associated terrestrial communication networks. Control operations in the orbital segment emphasize protection of satellites and their current and potential orbits. Finally, controlled access to the EMS includes protection of frequencies and bandwidths allocated for all space operations—including satellite C2, space surveillance, and satellite payload functionality. Ultimately, balanced integration of space control activities in all three segments ensures freedom of access, maneuver, and exploitation of space-based capabilities. Of note, and in accordance with the military's enduring purpose, space control operations persist in peacetime and war, demanding constant vigilance and preparedness in the event of aggression.

Under these conditions, Tables 3 through 5 list examples of key space control considerations in each space segment across the spectrum of conflict. Because space control is predominately defense-oriented, the activities listed represent potential defensive space control (DSC) measures. Furthermore, the actions listed are not standalone and instead represent multifaceted options for a layered and comprehensive approach to DSC across all space segments. However, the DSC considerations are notional and require additional exploration for nuanced analysis of validity. In this regard, the actions listed in the tables are not all-inclusive and merely serve to express the immense scale of military space control operations under the proposed model. ***The considerations listed in Tables 4 through 6 are conceptual and do not necessarily reflect existing or future capabilities***.

Table 4: Military Space Control Considerations in the Terrestrial Segment

Function[13]	**Assets / Regions**	**Control Options**	**Purpose**
Satellite C2	- AFSCN	- Physical protection of AFSCN sites - Cyber defense of terrestrial communication networks connecting AFSCN assets and other satellite C2 centers[14]	- Secure access to established (i.e., expected) satellite C2 locations for assured access and scheduling of satellite contacts - Ensure information confidentiality, integrity, and availability for satellite operations in orbital segment
Space Surveillance	- Terrestrial-based surveillance and MW sites	- Physical protection of SSN sites - Cyber defense of terrestrial communication networks connecting SSN assets and other surveillance centers (i.e., the JSpOC)	- Secure access to surveillance sites for SSA mission accomplishment - Ensure information confidentiality, integrity, and availability for surveillance operations to track and catalog activity in orbital segment (SSA)
Sustainment	- Launch sites - Launch vehicles - Satellite / launch vehicle manufacturing and storage facilities	- Physical protection of static launch sites; cyber defense of range operations and launch control centers[15] - Secure variety of launch vehicles and launch access points (airborne, mobile space launch) - Physical protection of satellite and launch vehicle manufacturing and storage facilities	- Secure access to specific launch locations for orbital access requirements[16] - Increase options for survivability and satellite reconstitution in orbital segment - Constellation development and sustainment; operational reserves

Source: Author's Original Work

The orbital segment, listed next, represents the focal point for all space control operations. Space control in the orbital segment focuses on the survivability of physical

[13] Terrestrial space assets located in theater AORs may also be considered for placement on the CCMD Area Air Defense Commander's (AADC) critical and defended assets lists (CAL and DAL, respectively). Under current constructs, nomination for CAL / DAL placement would originate from USSTRATCOM or JFCC SPACE based on mission requirements.

[14] This is an example of a critical integration point between defensive space control and cyber defense operations.

[15] Launch sites, launch vehicles, satellite manufacturing facilities, satellite C2 nodes, SSN assets and networks, etc. represent components of an infosphere's physical dimension. Thus, physical protection of these assets supports infosphere control measures.

[16] Launch site latitudes dictate range of viable orbits for satellite insertion—based on orbital inclination and attainable velocities. For example, launch sites nearest the equator (0 degrees latitude) are optimal for inserting satellites into geosynchronous orbit, whose orbital inclinations typically reside at 0 degrees. Furthermore, the earth's rotation is fastest at the equator, reducing the requirement for additional thrust to escape earth's gravitational field.

assets and orbital security. Both measures are directly associated with preserving space-based information collection and dissemination options.

Table 5: Military Space Control Considerations in the Orbital Segment

Function	Assets / Regions	Control Options	Purpose
Satellite Survivability	- Satellites	- Protection of assets (satellite hardening, on-orbit defender satellites [micro], decoys, etc.) - Enhanced SSA (ground- and space-based): Collision avoidance measures (increased satellite agility / maneuverability), onboard threat detection and autonomous response[17] - Disaggregation—expand constellations with multiple, smaller satellites[18]	- Ensure survivability of information systems within infospheres - Characterize orbital environment for change detection and threat assessment - Complicate adversary targeting; increase constellation robustness
Space-Based Information Collection and Dissemination	- Orbits	- Maintain clearance (from debris and/or other satellites) of nodal crossings and apogee[19] - Disaggregation of capabilities across multiple orbits	- Optimize maneuver options while conserving propellant—this allows for freedom of maneuver to access new orbits based on emergent collection and/or dissemination requirements - Redundancy for information collection / dissemination; complicate adversary targeting

Source: Author's Original Work

Finally, space control in the EMS ensures mission sustainment and connectivity between terrestrial and orbital operations, serving as the enabling feature of space control operations. Generally speaking, access, maneuverability, and exploitation of the EMS are defined in terms of frequency and bandwidth. Table 5 lists certain EMS protection considerations for space control.

---

[17] AFSPC now operates an integrated network of ground- and space-based surveillance sensors to provide greater awareness of man-made objects orbiting the earth.
[18] While disaggregation presents a viable option for the intended purpose, it also complicates defensive space control considerations and SSA requirements. In turn, this may create greater complexity for information control by increasing the reliance on networked systems and creating more refined degrees of information degradation.
[19] As a satellite moves around the earth, its orbit inevitably intersects the equatorial plane—twice. These intersection points are labeled the *ascending* and *descending* nodes. Due to extreme speeds and limited on-board propellant, satellite maneuvering—in a benign situation—is optimal at the nodes and apogee (an orbit's furthest point from earth and the point at which a satellite's kinetic energy is lowest).

Table 6: Military Space Control Considerations in the EMS Segment

Function	Assets / Regions	Control Options	Purpose
Information Collection and Dissemination	- SSN, Satellite C2, Satellite payload operations	- Monitor, detect, attribute electronic warfare (EW) attacks against space systems in orbital and terrestrial segments[20] - Frequency hopping, dummy signals, reserving alternate frequencies along allocated bandwidth, chattermark plans (synchronized between operational users and EW detection systems), etc.	- Maintain access to frequencies and bandwidths for information collection and dissemination in and through terrestrial and orbital segments.

Source: Author's Original Work

As inferred through the above tables, space control requires detailed awareness of activities across the entire space architecture; revealing the fundamental relationship between SSA, ISR, cyberspace, and all other space missions, specifically space control. From this conceptual relationship, a somewhat prescriptive model emerges that directly connects SSA activities with space control objectives. For the purposes of attaining space control (a defense-centric function), military SSA operations must be able to persistently *monitor* friendly and potentially hostile space assets and activities, *detect* changes in the environment, *characterize* the detected change, *assess* intent and purpose of the status change, and *mitigate* or *neutralize* hostile activity or its effects, as required—in all three segments (although the process is optimized for space surveillance).[21] The process extends from John Boyd's theoretical OODA loop model, as explained in Chapter 1.

- *Monitor:* Using a combination of space surveillance assets and other ISR resources (including those outside of the space community), DSC operations must orchestrate and execute persistent coverage of adversary and friendly activities in all three segments (a convergence of DSC, SSA, ISR, and cyberspace operations). The primary purpose of monitoring is to establish a baseline for strategic and operational environments. An on-going function, even after detection occurs.

[20] Interference detection systems and processes must be able to differentiate between unintentional electromagnetic interference (EMI) and intentional attacks (EW). While space control prioritizes EW, rapid resolution of both scenarios contributes to information control.
[21] The proposed space control process also integrates with space superiority operations, discussed next. However, the offensive character of space superiority drives a closer relationship to the doctrinal approach of find, fix, track, target, engage, and assess (F2T2EA, otherwise known as the "kill chain").

- *Detect:* The environmental baseline provides a reference point to distinguish expected from abnormal activity (e.g., a satellite's station-keeping maneuver executed beyond normal timelines or boundaries). Thus, detection involves recognition and notification of unexpected changes in the environment as they occur. Furthermore, the fusion of layered and diverse monitoring capabilities may help anticipate changes before (or while) they occur.
- *Characterize:* When a change is detected, the onus shifts to understanding the nature of the change (e.g., was the change minor or did it involve a significant shift in operations or procedures? Does the change influence readiness levels or capability?). Additionally, the change is contrasted with activity in other segments of the architecture and broader activities in other operational domains.
- *Assess:* Upon characterizing the change, analysis moves toward determining the purpose or intent. Was the change driven by hostile intent? Was the change a result of environmental factors or benign system failures? Was it the result of a deliberate shift in the space architecture to accommodate other planned activities? What is the status of friendly assets—have any friendly space assets or units reported abnormal activity? (A continuing consideration throughout the process.)
- *Mitigate / Neutralize:* If the change affects friendly systems, execute established or ad-hoc (passive and/or active) mitigation options. If the change is hostile or aggressive, execute appropriate DSC options to neutralize threat (may involve coordination of activities in other domains and other organizations).

A Word on Space Superiority

Space superiority involves a relative advantage in domain control to meet strategic needs. Therefore, space superiority necessitates a greater application of offensive capabilities (orchestrated under the umbrella of comprehensive OSC strategies and operations) to actively deny an adversary's required use of space. In addition, while the character of modern warfare demands a certain level of space control, it may not

always require the additional attainment of space superiority, as described above.[22] Table 6 highlights considerations for attaining space superiority by virtue of coordinated and layered OSC-related operations across each space segment. Again, ***the considerations listed in Table 7 are conceptual and do not necessarily reflect existing or future capabilities***.

Table 7: Military Space Superiority Considerations Across All Space Segments

Function	Assets / Regions	Superiority Options	Purpose
Deny Adversary's Required Access to Space	- (Terrestrial) Space surveillance sites, satellite C2 nodes, space operations centers, launch sites, satellite manufacturing sites, etc. - (Orbital) Satellites / Orbits - (EMS) Frequencies / bandwidth (surveillance, C2, space-based information collection and dissemination, etc.)	- Standoff strikes (air strikes, cruise missiles), SOF engagement, cyber attacks, etc. on enemy space assets in terrestrial segment - Orbital and DA-ASAT attacks against critical constellations or specific satellites; space "blockade" against orbital nodes and/or apogees to interfere with enemy satellite maneuver options and orbital access points - EW and cyber attacks against adversary frequencies and bandwidths; cyber attacks	- Deny adversary access, maneuverability, or exploitation of space-based capabilities (as dictated by his strategy)

Source: Author's Original Work

Collectively, space control and space superiority operations embody the true nature of space warfare. Space control, contingent upon the preservation of access, emphasizes DSC operations conducted through the proposed process of monitoring, detecting, characterizing, assessing, and mitigating or neutralizing harmful activity. Space superiority, the intended outcome of denying an adversary his required use of

[22] This condition may hold true for a spacefaring nation at war with a non-space power. As the essence of strategy implies, however, space superiority is a necessary objective in the event of war with a peer or near-peer space power.

space, is dependent upon the sustainment of space control. Furthermore, while closely associated with space control processes, space superiority emphasizes OSC operations and is therefore more closely aligned with the traditional "kill chain," or F2T2EA, construct. Most importantly, *space control and space superiority demand the deliberate integration and orchestration of OSC, DSC, SSA, ISR, and cyberspace across all three segments of the space architecture*.[23] Ultimately, a comprehensive space control strategy illustrates the complexity of an overarching information control strategy and the requirement to elevate information control to a prominent position in national security.

Synchronization of Space and Information Control

The proposed concepts of space control and information control synchronize under their interdependency. Through implementation of a distinct information control strategy, space and cyberspace components cooperatively plan and execute domain (infosphere) control operations in coordination with national and theater campaigns.[24] In this regard, placing the proposed space control model under an overarching information control strategy addresses two critical imperatives: prioritization and coordination of resource allocation and, more importantly, the ability to recognize and prevent infosphere degradation—the bedrock of information control.

First, the sheer scope of space control considerations (involving integrated OSC, DSC, SSA, and cyberspace functions), combined with limited resources, creates a need for prioritization and cross-domain coordination. Prioritization of DSC occurs through the identification of satellites or constellations (space-based information collection and/or dissemination systems) that support imbedded strategic, operational, and tactical information requirements and form the backbone of associated infospheres. By extension, the prioritization of critical information assets allows for the identification of relevant *threat* systems that are capable of denying friendly capabilities, thereby

[23] Because space control influences operations at all levels of war, the integration of each function is scalable to meet specific requirements. For instance, tactical and operational planners will integrate OSC, DSC, SSA, ISR, and cyberspace for specific strike operations just as strategists will incorporate a similar structure in support of overall campaigns.

[24] Space architectures and operations encompass multiple CCMDs at any given time. Therefore, space control and information control strategies simultaneously involve global and regional infospheres, requiring their own separate campaign effort. In this sense, national and theater campaigns help set priorities for the broader, strategic endeavor of information control (via space and cyberspace control in each infosphere).

improving the ability to anticipate and counter adversary OSC operations. In reference to the space control process highlighted previously, prioritization enhances the effectiveness and responsiveness of *monitoring* and *detecting* friendly and adversary space activity in all three segments. Subsequently, prioritization enables development and implementation of appropriate response options—across all domains—based on focused monitoring and detection.

Relatedly, the second, more strategic benefit of connecting the proposed space control considerations with information control is allowing the joint force to establish and recognize thresholds for unacceptable information degradation. In the absence of such integration, all space systems are considered a priority, placing an insurmountable burden on planning and executing space control operation. Most significantly, a lack of integrated space, cyberspace, and information control strategies prevents anticipation or assessment of mission impact due to loss of control, potentially leading to strategic failure. By linking and prioritizing space systems with information requirements, senior decision-makers, joint planners, and warfighters can recognize when degradation of space systems will affect strategy, campaign, operation, and/or mission accomplishment.[25] *In operational terms, this provides context for determining when space control is achieved, when it is lost, and how to gain it*. From a strategic perspective, it provides a broad metric—in conjunction with cyberspace control—for assessing whether the joint force can continue with its desired strategy. Just as importantly, synchronizing space, cyberspace, and information control may allow planners and warfighters to determine *where they can take a hit in space* and continue to function as designed (i.e., through determining minimum force requirements in space).

[25] For example, at the tactical level, satellites—and their supporting architectures—delivering critical information for a particular strike package will garner enhanced protection for the duration of the mission. This provides a prioritization scheme for space control planners to ensure freedom of access, maneuver, and exploitation of the critical SFE functions enabling the strike operation. National and joint planners may then identify specific threat activity that may deny SFE access. Tactically, if space system degradation does occur, planners will have greater insight into their ability to fulfill strike mission objectives. Strategically, the amalgamation of space control operations at the tactical and operational levels provides assessment of the ability to continue projecting and employing force as desired. This level of coordination requires globally networked communications, generating yet another forcing function for the integration of space and cyberspace operations under an information control strategy.

Ultimately, adopting an information control strategy concurrently provides the joint force with a guideline for cohesive transformation and a unifying vision for US space operations; two interrelated yet distinct problem sets in the US defense establishment. In terms of transformation, operational and tactical realities influence a new strategy's feasibility. Moreover, an existing strategy generates the framework upon which military doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) coalesce. Because DOTMLPF describes the military's overall capability in a certain mission area, it serves as a useful tool for analyzing current capacity. As revealed in Chapter 4, the US space infrastructure did not develop under the precepts described above and thus executes its mission with DOTMLPF that satisfices an outmoded paradigm. In essence, current space DOTMLPF may not be postured to effectively conduct space warfare and achieve space control in the pursuit of information control. The analysis therefore concludes with an assessment of space DOTMLPF and recommendations for transformation.

Military Space DOTMLPF—Assessment for Space Control

According to the US Army Capabilities Integration Center (ACIC), "DOTMLPF is a problem-solving construct for assessing current capabilities and managing change."[26] Institutionally, the greatest challenge to US military transformation may lie in the archaic policies and strategies that drive its space DOTMLPF requirements and operations (specifically from the USAF perspective). Indeed, the ability for current US space DOTMLPF to accommodate the proposed paradigm may represent a critical barrier to military effectiveness in the twenty-first century. In addition, the transformation required to attain space control inevitably demands an equal shift in the intelligence community. Thus, the DOTMLPF review also includes a brief commentary on intelligence for space.

Doctrine

Although discussed previously, a brief synopsis of US joint and service doctrine regarding air, space, cyberspace, and information operations follows. Air power doctrine,

---

[26] US Army Capabilities Integration Center, "What is DOTMLPF?," http://www.arcic.army.mil/AboutARCIC/dotmlpf.aspx, (accessed 23 April 2015).

codified in Air Force Doctrine Document 1 (AFDD 1), incorporates air, space, and cyberspace under one holistic concept of *airpower*. A nuanced shift from earlier notions of *aerospace* power, combining the three domains into one element of military power inadvertently creates an identity crisis in all three. Are functions of air, space, and cyberspace cohesive to the point where a single doctrine can adequately define their distinct roles and maximize their potential? A partial answer to this question is found in the implementation of airpower doctrine into joint operations and organizations.

Operationally, a conflated airpower doctrine generates a false kinship between the definitions of, and authorities for, air, space, and cyberspace superiority. In many respects, this integration occurred as a result of geopolitical and institutional motivations. Since the end of the Cold War, no imminent threat existed in space, and the requirements for gaining or maintaining space superiority proved minimal (i.e., space superiority was a presumed condition). Additionally, the USAF capitalized on post-Cold War realignments by claiming domain ownership through its traditional aerospace paradigm. Consequently, theater air force commanders (i.e., the COMAFFOR and oftentimes the JFACC) are now given the responsibility for gaining and maintaining air and space superiority by virtue of airpower doctrine. As argued earlier, however, this perspective ignores the functional relationship between space and cyberspace and impedes the implementation of a larger information control strategy, which exceeds the resources and authorities of any one geographic combatant commander. Moreover, the magnitude of space control operations—as presented here—is such that a theater COMAFFOR or JFACC cannot effectively plan or execute space operations, much less gain or maintain space superiority in its truest sense.

Rather than affiliating space with air operations, joint and service doctrine should emphasize the criticality of information control across traditional warfighting domains. In so doing, space and cyberspace control assume a prominent position in the new warfighting paradigm—indeed, space and cyber warfare are tantamount to Information Age warfare. This information control framework offers a counterpoint to the traditional assumption that "space capabilities are inherently cross-domain integrated," instead suggesting that integration occurs through the deliberate establishment of information requirements and prioritization of space and cyberspace control operations to ensure

access.[27] The new paradigm readjusts relationships between air, space, and cyberspace and creates an imperative for unified space and cyberspace control strategies in support of information control. Doctrinally, the primary focus of USSTRATCOM, AFSPC, and JFCC SPACE shifts to controlling access to space in support of global and theater SFE requirements within an information control campaign, distinct from, yet coordinated with, theater campaigns. In adopting this approach, theater COMAFFORs and/or JFACCs dedicate their resources to *air* operations, while space and cyberspace operations combine under a separate entity with objectives that transcend (but include) theater information requirements.[28]

Organization

With AFSPC and JFCC SPACE serving as the prominent executors and orchestrators of military space operations, their organizational structures offer insight into the military's current posture in space, particularly for space control. From service and tactical perspectives, AFSPC's 4th and 76th Space Control Squadrons (SPCS) perform OSC in support of warfighter requirements. The 16th SPCS, the USAF's only active duty DSC unit, conducts operations representative of prevailing DSC missions. From an operational level C2 perspective, the Joint Space Operations Center (JSpOC), modeled in accordance with the USAF's AOC construct, represents the operational element of JFCC SPACE. The new theoretical framework presented earlier asserts that space control requires the integration of OSC, DSC, SSA, ISR, and cyberspace operations across all three segments of the space architecture. Tactical and operational space control structures and missions are therefore assessed through this standard.

At the tactical level, USAF OSC and DSC operations fall under AFSPC's 21st Space Wing and are optimized for exploiting specific aspects of the space architecture. According to available fact sheets, 4 SPCS and 76 SPCS "[operate] and [maintain] the

[27] AFDD 3-14, *Space Operations*, 19 June 2012, 2.

[28] Airborne platforms will inevitably "plug" into space and cyberspace networks, but so will naval and land assets. Consequently, the JFACC is not responsible for establishing or controlling access to infospheres—infosphere control, fundamentally, is attained through space and cyberspace control. At a minimum, space and cyberspace control, being global in nature, should fall under the authority of USSTRATCOM, USCYBERCOM, and JFCC SPACE (based on existing structures). The JFACC, along with all other theater component commanders, is instead responsible for identifying information requirements, determined through strategy and resultant decision-making processes.

Counter Communications System," and "[deploy] globally to conduct mobile and transportable space superiority operations as tasked by the Commander, JFCC SPACE."[29] The 16 SPCS operates ground-based systems designed to "detect, characterize, geolocate and report sources of radio frequency interference on U.S. military and commercial satellites in direct support of combatant commanders."[30] The three units provide highly effective, niche capabilities for national and theater commanders.

A cursory glance at the JSpOC's structure indicates that space control operations may not be planned, executed, or assessed in accordance with the proposed concepts. First, the JSpOC is comprised of six divisions: Strategy / Plans, Combat Operations (COD), SSA, ISR (ISRD), Operations Support (OSD), and the Unified Space Vault (USV). According to USSTRATCOM and JFCC SPACE publications, the USV "conducts various classified and unclassified Defensive Space Control, Offensive Space Control, and [SSA] missions."[31] The SSA Division provides operational C2 of the SSN and maintains a catalog of all man-made earth orbiting objects known as the Satellite Catalog, or SATCAT. The SATCAT provides a point of reference for predicting potential collisions in orbit, and the JSpOC actively monitors and notifies military and civilian users of such events. While COD "conducts command and control over the execution phase of operations and provides information on tasking responses to the JFCC SPACE commander," division operations primarily center on monitoring constellation status and coordinating SFE requirements with national and theater users.[32] From a cyberspace integration perspective, coordination at the JSpOC occurs primarily in ISRD, while the JFCC SPACE J6 provides a staff-level interface. No division is directly responsible for establishing or coordinating terrestrial protection measures with CCMDs.

Viewed together, tactical space control operations and operational level space C2 are organized and concentrated in ways that assume a certain level of domain superiority

[29] United States Air Force Space Command, "4 SPCS Fact Sheet," http://www.peterson.af.mil/library/factsheets/factsheet.asp?id=4707 (accessed 25 April 2015).
[30] United States Air Force Space Command, "16 SPCS Fact Sheet," http://www.peterson.af.mil/library/factsheets/factsheet.asp?id=8403 (accessed 25 April 2015).
[31] United States Strategic Command, "JFCC SPACE Fact Sheet," http://www.vandenberg.af.mil/library/factsheets/factsheet.asp?id=12579 (accessed 25 April 2015).
[32] United States Strategic Command, "JFCC SPACE Fact Sheet," http://www.vandenberg.af.mil/library/factsheets/factsheet.asp?id=12579 (accessed 25 April 2015).

already exists. Moreover, current space control operations are limited in scope and are not typically infused across all space segments. While extremely capable in their own right, the organizations are not postured to plan, execute, or assess the comprehensive space control measures outlined earlier. This is not surprising, as reviews of space doctrine, policy, and history indicate that space control is indeed *not* the current operational priority, or at least operationally aligned with this analysis. Organizations and missions evolve to accommodate existing paradigms (and strategic landscapes), and space control is currently accomplished through disparate units specializing in unique tasks rather than through a unified effort driven by a strategic imperative.

One possible organizational structure for conducting operational C2 and tactical space control operations is provided in Figure 11. The figure highlights organizational and functional integration of each space control discipline along with a series of liaison elements to coordinate space control initiatives with cyberspace organizations, CCMDs, and commercial or civil entities.[33] To incorporate the entire space architecture into the organizational scope, each section (OSC, DSC, Surveillance, and Intelligence) facilitates respective operations in each space segment. Of note, each segment team plans and coordinates activities corresponding with the considerations listed in Tables 3 through 5 and contributes to the process of monitoring, detecting, characterizing, assessing, and mitigating harmful activity. The notional structure is scalable, meaning it could apply to a tactical unit forward deployed and connected back to an equivalent C2 structure at JFCC SPACE or USSTRATCOM.

[33] JFCC SPACE could function as a de-facto Joint Functional Space Component Command (JFSCC) for each geographic CCMD. In this capacity, JFCC SPACE (or the JSpOC) would facilitate component-level liaisons with each GCC to coordinate planning efforts, missions, objectives, and joint targeting boards. Space control objectives would be developed, executed, and coordinated by JFCC SPACE and remain linked with strategic and theater information control strategies, ensuring synchronization with cyberspace activities to ensure proper establishment and control of infospheres.

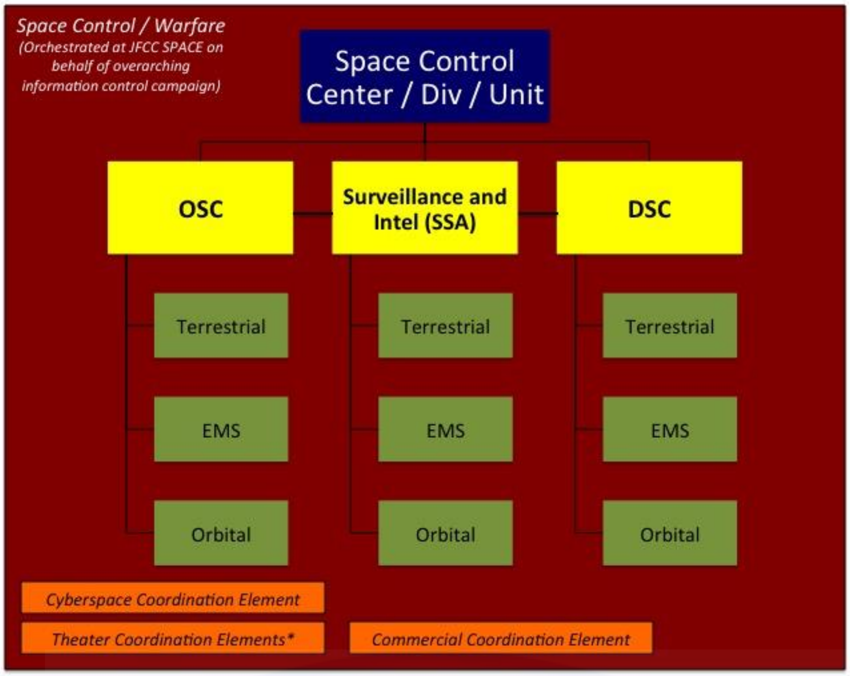

Figure 11: Notional Space Control Organizational Structure (Operational and Tactical)
Source: Author's Original Work

The overall conduct of space warfare parallels the space control portion of the information control diagram first shown in Chapter 3. Therefore, the immediate objective of this new organizational structure is space control for the explicit purpose of assuring access to required SFE capabilities, *which in turn fulfills the space aspect of infosphere and information control*.

Training

The primary concern of training is the establishment and sustainment of a space control tradecraft within the operations community. Doctrine and organizational structures influence training priorities, and they are evident in the space community's training regimen. Today, most tactical training programs focus on maintaining the health and status of various operational systems, and rightfully so. However, threat detection, coordination, and processing typically constitutes a secondary (or lower) training goal, while conceptualizing how these systems integrate into the joint fight designates a tertiary

priority, and only abstractly.[34] Furthermore, only a handful of military space professionals have access to advanced orbital mechanics training, a fundamental discipline for understanding how to maneuver in the space medium. In short, due to historical, political, and cultural factors, the space control tradecraft has atrophied since the end of the Cold War.[35] As Sun Tzu noted, "if officers are unaccustomed to rigorous drilling they will be worried and hesitant in battle; if generals are not thoroughly trained they will inwardly quail when they face the enemy."[36] Indeed, former USAF Historian C.R. Anderegg's quote at the opening of the chapter is a prescient warning for military space strategists and tacticians.

One blatant example of the current warfighting paradigm and the inertia built against advancing a comprehensive space control tradecraft lies in the assignment and purpose of the USAF's only active duty space aggressor squadron, the 527 SAS. The 527 SAS falls under Air Combat Command rather than AFSPC and exists to improve joint warfighter resiliency in degraded EMS environments (yet another example of the current space control focus). While important for operations in terrestrial domains, a lack of dedicated space aggressors for holistic space control operations diminishes the space community's ability to change its culture and develop relevant tactics, techniques, and procedures (TTP)—or identify capability gaps—for space and information control. Subsequently, space control training concepts should extend into all service and joint warfare training programs, merging concepts of operations and expressing the joint imperative of comprehensive information control. A lack of skill sets and joint response options across the space architecture will invariably lead to failure in future wars fought within complex infospheres against near-peer competitors.

Materiel

Perhaps the most revealing component of the DOTMLPF framework rests in materiel as it unveils the dichotomy of actions versus words. From an acquisitions standpoint, two realities infer an institutional acceptance or assumption that US space

---

[34] Similarly, awareness of space operations (capabilities and limitations) in other military communities—*including the USAF*—is severely lacking, revealing a significant rift in the joint force's ability to uniformly appreciate the nuances of information control and the requirements for transformation across all services.
[35] To reiterate, this issue is not confined to the space community—it is a DoD responsibility.
[36] Sun Tzu, *The Art of War,* trans. Samuel B. Griffith (London: Oxford University Press, 1963), 66.

superiority is a default status. First, the USAF is acquiring and fielding systems that increasingly rely on networked communications to function (i.e., AOCs and fifth-generation fighters), perpetuating outmoded expectations for the continued availability of space capabilities. Second, and to the immediate issue, the USAF prioritizes its space budget for more sophisticated SFE capabilities, supporting the deceptive belief that space superiority is a function of superior technology. For example, the USAF's 2013 Budget Overview captures prevailing assumptions of space control and superiority when it explains, "Through the Space Superiority Core Function, Airmen provide space capabilities that enhance the DoD's ability to navigate accurately, see clearly, communicate confidently, strike precisely and operate assuredly."[37] The $9.6 billion allotted for USAF space operations addresses the Air Force's continued acquisition strategy for resilient, survivable, flexible, and responsive SFE capabilities as an approach to attaining space superiority.[38] In contrast to air and cyberspace acquisition goals, however, no mention is made of budgeting for robust space control capabilities to mitigate emergent threats in the domain, sustain space capabilities in hostile environments, or deny adversary access.[39]

Leadership / Education / Personnel

Combined, leadership, education, and personnel components address skill sets and proper placement rather than the quality of individuals. More than any other aspect, having the right combination of leadership, strategic awareness, and technical prowess can help create the requisite changes within the DOTMLPF structure. Conversely, allocating personnel with inadequate backgrounds only promulgates the inertia built from decades of operating under uninhibited conditions in space. At the JSpOC, for instance, an unofficial review in 2013 of company grade officers assigned to COD unveiled that

[37] United States Air Force, *FY 2013 Budget Overview* (Washington, DC: Office of the Deputy Assistant Secretary of the Air Force [Budget], February 2012), 41.
[38] United States Air Force, *FY 2013 Budget Overview*, 44.
[39] Recognition of the growing threat environment may generate future budget considerations for increased space control spending, however.

over 50 percent of officers entered the C2 unit without any prior space operations experience (instead, they transitioned directly from nuclear operations).[40]

Without dedicated cadre of space warfare specialists, appropriate recognition *and articulation* of space control capabilities, limitations, and susceptibilities across the space community (*and joint community writ large*) is difficult. Just as significantly, the lack of proper expertise in key positions reduces the organizational capacity to *implement* innovative processes that counter the dominant space culture. In his thorough investigation on military innovation, Stephen Rosen concluded, "Peacetime innovation has been possible when senior military officers with traditional credentials, reacting . . . to a structural change in the security environment, have acted to create a new promotion pathway for junior officers practicing a new way of war."[41] To make transformative innovation "stick," leaders rely on experts who understand the nuances of existing paradigms and can transpose new concepts upon them to evaluate the need for change.[42] Thus, a deliberate training, education, and placement program is necessary for building a cadre that can evaluate, articulate, and implement innovative concepts across the space community and joint force.

Facilities

Future space operations will require modern facilities that enhance training, incorporate emerging cyberspace defense concepts, and integrate physical security commensurate with space control requirements in the terrestrial segment. For example, the development of simulators for wargaming, TTP development, and TTP validation will prove instrumental for advanced training, particularly for operational-level scenarios supported by space aggressors. The combination of robust space control simulators and complex scenario development by space aggressors would indicate a substantial shift in current thinking regarding space power employment.

---

[40] Based on JSpOC COD manning review conducted by Lieutenant Colonel Matthew Cantore (Deputy Chief, Combat Operations Division) and Major Casey Beard (Chief, Defensive Operations Branch), Spring 2013.

[41] Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military*, (Ithaca, NY: Cornell University Press, 1991), 221.

[42] For further analysis on individual innovation in organizations, see Clayton M. Christensen, *The Innovator's DNA: Mastering the Five Skills of Disruptive Innovators*, (Boston, MA: Harvard Business Review Press, 2011), 27.

From a DSC viewpoint, protection of critical space facilities requires coordination with cyberspace and CCMD components. Greater incorporation of cyberspace defense with DSC operations in the protection of terrestrial communication networks supporting space facilities is essential. Physical protection of space facilities currently manifests itself through designation of security protection levels but may also include the identification of geographically distributed space facilities in CCMD critical and defended asset lists (CAL and DAL, respectively)—in fulfillment of space control requirements. Adopting an information control strategy that incorporates combined space and cyberspace control measures will provide the requisite guidelines for creating a robust protection scheme for terrestrial assets.

Intelligence Apparatus

The DOTMLPF components above all focus on military space, but the same categorizations translate over to the national intelligence apparatus. While not typically included in the DOTMLPF structure, the capacity for the intelligence community to provide exquisite intelligence *for* space rather than *from* space warrants a separate dialogue. The proposed shift in strategic, operational, and tactical requirements will necessarily drive transference in the national intelligence community. In its most basic form, intelligence in this new construct will involve rapid, detailed threat analyses over all three segments of the space domain. Needless to say, the strategic adjustment will generate a profound burden on the national intelligence apparatus that merits further investigation.

Final Synthesis and Conclusion

The terms *space control* and *space superiority* instigate different reactions from different communities, sparking intense debate as to the proper military footprint in the domain. Under the new paradigm for Information Age warfare, the two terms take on a new perspective, and a renewed importance. First, the military's role in space is to contest or control access to the domain and its unique capabilities in support of political objectives. Second, in the twenty-first century, the US military relies on global, near-instantaneous, and accessible information to project and employ force. A new concept of

warfare elevates the importance of controlling information access to the forefront, demanding a shift in traditional joint force priorities. Space architectures form the foundation of global information networks and therefore represent the focus of space control operations in the Information Age.

Space control operations ensure freedom of access, maneuver, and exploitation of the terrestrial, orbital, and EMS segments comprising the space architecture. Control is measured by the ability to prevent others from denying that freedom and is therefore defense-oriented. Procedurally, space control seeks to monitor, detect, characterize, assess, and mitigate threats in any and all segments of space. Space superiority, reliant on the attainment of space control, is relative as compared with an adversary's ability to access (or control) space in fulfillment of his strategy. Superiority necessitates offensive and defensive measures to deny an adversary's access to all space segments while securing one's own and tends to follow the more traditional F2T2EA process.

Information control establishes the guiding parameters for space control priorities and assessments, providing a unifying strategy for warfare in all domains. Enhanced protection is given to those assets supporting specific tactical, operational, and strategic information requirements, demanding a much deeper level of cross-domain integration than ever before. Furthermore, assimilating space control with information control creates new metrics for assessing attainment or loss. If access to mission-specific space systems is maintained across all segments, then space control is attained for the purposes of information control. If satellite degradation occurs to the point where mission accomplishment is no longer possible, then space control is lost, even if only temporarily (or tactically). At the strategic or campaign level, the amalgamation of multiple tactical losses may reduce or prevent the joint force's ability to project or apply force as desired. Maintaining the fidelity to recognize and prevent such degradation constitutes the hallmark of space and information control strategies.

It is for this reason why space control is not simply the space community's problem. The space control methodology presented in this chapter offers a glimpse into the complexities of such an immense undertaking, one that far exceeds the capabilities of extant space DOTMLPF and directly challenges concepts of war in other domains. Because of its cross-domain implications, the pursuit of space control is irrelevant

without a joint imperative that drives it. An information control strategy provides a trajectory for transforming an Industrial Age military into an Information Age force and establishes an immediate impetus for space (and cyberspace) control. In turn, a space control strategy gives much-needed context for assessing and transforming space DOTMLPF and facilitates seamless integration of cross-domain operations. Thus, adoption of a space control strategy is contingent upon acceptance of a new way of warfare that prioritizes information control across the entire joint force. In short, space control initiatives without a joint imperative will fail, and a joint force that fails to appreciate the intricacies of space and information control will not be able to preserve its desired way of warfare in the future.

CONCLUSIONS

Humans are finite and fallible beings. Human nature signifies the persistent response to this condition and strives to compensate for its deficiencies by finding or creating stability in chaotic environments. Stability is gained by generating predictability through the perception of situational control or influence. Strategy exists to fulfill this fundamental impulse.

Conflict, in various degrees, initiates when human interests intersect. War resides at the most extreme end of conflict’s spectrum, as it encapsulates and rectifies the fears, uncertainties, desires, and emotions of the masses. Military strategy, a derivation of national (or grand) strategy, exists to insert stability and situational influence in war. The competitive element of conflict (and, by extension, war) values the opponent’s destabilization by removing his ability to control or influence outcomes. In so doing, one gains an advantage over an opponent by manipulating human nature and exploiting the human condition. Thus, stability in war exists by gaining relative advantages to influence outcomes commensurate with war’s purpose. Once again, stability through advantage and control is a central aim of strategy.

War, however, is a dynamic and unpredictable phenomenon, propelled by imperfect and self-preserving beings. In the insatiable pursuit of stability and control, humans continually absorb and process information and evaluate perceived risks through the filter of their interests. The end result is informed decision-making and, ultimately, appropriate action. Strategy, then, provides the necessary scaffolding for determining required decisions and the information needed to support them. Therefore, a critical potency is generated in the proper balance of strategy, decision-making, and information. In conflict (and war), the priority must remain fixed on protecting one’s strategy-decision-information triumvirate and disrupting the enemy’s.

Western military history supports such a narrative. From the Roman Legion to Napoleonic armies, from Moltke’s general staff to the current US military, strategists have developed approaches to warfare corresponding to the expected quantity and quality of available information. As armies, destructive power, range, and speed increased, the ability to orchestrate activities across continental regions took center stage, changing

expectations for war’s conduct. By the early 1900s, key breakthroughs in communication technology were inevitably incorporated on the battlefield, a manifest of human nature and strategy. Soon, war took on a third dimension as air power arrived on the scene, elevating the importance of long-range communication capabilities to exploit the new advantage. Radios and radar filled this initial role, and by the 1960s, space-based capabilities introduced the possibilities of worldwide collaboration, forming the mainstay of global information collection and dissemination networks. In each instance, these information technologies were interlaced in war by virtue of strategy (determining their value) and decision-making requirements (assigning their utility). Strategy and human nature, it seems, transcend ages.

The characteristics of human nature, strategy, and their combined pursuit of advantage and influence brought about advancements in information technologies that eventually changed perceptions, expectations, and values in warfare. In this regard, the space age marked a significant milestone in human history. A product of the Industrial Age, space capabilities challenged existing methods of strategic intelligence, diplomacy, communications, commerce, military targeting, et cetera—in essence, space capabilities enabled a new approach to national security. As the Cold War progressed, the US space infrastructure remained a bulwark of nuclear deterrence, and was thus characterized as a strategic asset. By 1991, Desert Storm and the end of the Cold War revealed the true potential of space-based ventures, representing a symbolic transition point in the world’s conception of information. In short, space capabilities, the apex of the Industrial Age, helped usher in the dawn of the Information Age and a new paradigm.

With a sudden abundance of information (and the abrupt change in geopolitical climates after the fall of the Soviet Union), decision-makers placed greater emphasis on developing new, more sophisticated information systems. Following the space age, advancements in terrestrial-based computer technologies emerged, and by the 1980s, the concept of cyberspace took root in the form of computer networks. Cyberspace greatly enhanced the capacity for collaboration and coordination across the globe, and the end of the Cold War enabled rapid proliferation of space and cyberspace capabilities across a global market economy. By the 1990s, space and cyberspace systems were intertwined

in a complex yet complementary array, inadvertently forming the backbone of global information environments, or *infospheres*.

However, the lack of a near-peer competitor after the Cold War reduced the incentive for the US military to understand the intricacies of the capabilities that enabled it to operate as effectively as it did. The absence of an existential threat allowed the US military to conduct its operations around the globe with minimal resistance, and the propagation of information technologies created a situation in which the military could exploit the benefits of net-centric warfare without having to contend with its potential ramifications. Moreover, the essence of strategy dictated that the US military focus on leveraging advantages to disrupt its weaker opponent's physical balance. In the process, joint forces (and society writ large) inadvertently accepted a wholesale dependency on information technology for national prosperity and security while carrying a lesser regard for the details that enable them.

Thus, instead of converging, space and cyberspace operations and strategies diverged, indicative of existing paradigms. As the late 1990s approached, space force enhancement (SFE) capabilities—now closely aligned with conventional warfare—thrived with relatively little external resistance, while cyberspace quickly evolved into a new domain of warfare. As a result, less operational emphasis was placed on securing access to space in non-permissive environments while additional attention and resources were allocated for cyberspace, the "new" information domain. At the same time, the US military remained fixed in an Industrial Age mindset, placing greater priority on terrestrial operations while viewing space as an extension of the air and cyberspace as a supporting (and nebulous) infrastructure.

The United States assumed a new set of values and expectations in warfare after the turn of the century. In a matter of a decade, the US military was able to exploit space and cyberspace capabilities in relatively permissive environments that enabled it to reduce risk to friendly forces, deliver incredibly precise firepower anywhere on the globe, and minimize collateral damage. Consequently, the US military's desired way of warfare in the twenty-first century—guided by its political authorities—is now described as *the concentration of lean, disparate, and geographically dispersed units at a specific time*

and place for precision engagement. As such, the focus in space and cyberspace remains on providing support to terrestrial operations in accordance with the desired approach.

Viewed through the perspective of human nature, the stage is set for a potentially devastating blow to US military strategy. Since the end of the Cold War, the proliferation of information technologies created a certain level of technological parity beyond the realm of superpowers. State and non-state actors alike benefited from the Internet and space-based capabilities. Meanwhile, the United States existed as the only remaining superpower, forcing it to divest its resources across a range of contingencies. The confluence of technical commerce and US hegemony created the current situation in which potential adversary's now focus on circumventing or undermining US asymmetrical advantages.

At the same time, the US defense establishment confidently progresses its notion of warfare without fully appreciating the capabilities, limitations, and susceptibilities of the space and cyberspace networks (i.e., infospheres) enabling it. Weapons programs like the F-35 Lightning II, designed to exploit net-centric advantages for its functionality, portray an obsolete mindset that presumes accessibility to global information networks in contested environments. Unfortunately, the procurement and implementation of such systems are not accompanied by changes in warfighting doctrine that assure combined access to space and cyberspace. In fact, the US military space infrastructure—bound so long by Cold War politics, prohibitive treaties, and fluctuating strategies—is not designed to systematically secure access to space in a non-permissive environment. Indeed, technical advantages and freedom of action that shaped US expectations of warfare are now relics of a temporary phase in geopolitics and yet still define warfighting policy, strategy, and doctrine. In sum, the joint force is not postured to preserve its desired way of warfare in the Information Age (a strategic oversight, but one explained by the prevailing mindset).

Therefore, a new mindset and way of warfare are required to preserve America's ability to operate as desired. *The US military must deliberately identify, prioritize, and secure critical space and cyberspace infrastructures (infospheres) that enable its desired way of warfare*—the core of an information control strategy and an imperative for the entire joint force. Implementation of such an approach first requires adoption of a new

paradigm that perceives global information systems as the lifeblood of national defense and considers the protection of technologies that collect and disseminate global, near instantaneous, and accessible information as the preeminent objective. Moreover, the paradigm shift and subsequent change in warfighting strategy must occur across the entire defense establishment, influencing the doctrine and behavior of all services by elevating information control and superiority to *foundational requirements* prior to operating in and/or through any domain. Ultimately, information control is a global endeavor that cannot be achieved through the traditional emphasis on regional campaigns. While disruptive, such a shift is necessary for maintaining America's advantage in tomorrow's threat environment.

The concept of information control covers all three levels of war but is best defined at the operational and strategic levels. At the operational level, the new way of warfare involves coordinated actions that assure freedom of access, maneuver, and exploitation of the space and cyberspace infrastructures forming the physical and information dimensions of infospheres. The proper balance of strategy, decision-making, and information provides requisite prioritization for this endeavor, as strategy reveals decision-making parameters, which in turn determine information requirements. Consequently, information control exists to secure freedom of access, maneuverability, and exploitation of established infospheres—*commensurate with one's strategy*—and the ability to prevent others from denying that freedom. Information requirements, when matched against information collection and dissemination capabilities in space and cyberspace, create the baseline for prioritized defense.

At the strategic level, information control accounts for the realities of warfare in space and cyberspace. Due to their global and entangled arrangements, complete destruction of an entire space and cyberspace network is essentially unobtainable. However, significant disruption or degradation to space and/or cyberspace infrastructures is not only possible, it is *expected*; particularly as more adversaries field advanced counterspace systems and cyber attack capabilities. Therefore, the onus falls on strategists to identify, anticipate, assess, and prevent the level of infosphere degradation that inhibits their desired way of warfare. An overarching information control strategy serves this very purpose.

The essence of strategy indicates that control is essential, but superiority is the key to victory. Sun Tzu and J.F.C. Fuller emphasize the preeminence of attacking the enemy's strategy for success, and in the Information Age, denying an enemy's access to the information systems needed to fulfill his strategy may serve as the fulcrum upon which victory lies.[1] Hence, information superiority—a relative condition of control predicated on offensive action—implies that one side is able to control access to the infospheres enabling strategy while the opponent is unable to exert the level of control required by his strategy. Strategically, information superiority therefore involves the ability to maintain information control—relative to one's informational needs—while denying the adversary's ability to recognize and prevent degradation of his own infospheres relative to the needs of his strategy.

As shown, information control and superiority demand the integration of global space and cyberspace control and superiority strategies. However, in many respects, warfare in cyberspace is now an accepted reality, while space control and space warfare spark political controversy. Furthermore, the divergence of space and cyberspace operations and functions creates a disjointed approach to warfighting that can only be reconciled through a new paradigm and unifying strategy. By recognizing information control as a global endeavor that views space and cyberspace operations as functional equivalents, military space and cyberspace operations may unite under a common strategy that gives impetus for mutual control of the infospheres they form.

Such a complex and far-reaching strategy requires a new force structure to devise and orchestrate global information control strategies and coordinate actions across multiple combatant commands. In this regard, a new functional combatant command is warranted, replete with authorities, responsibilities, funding, and resources to adequately operationalize the new paradigm. The combatant command assumes responsibility for the global fight for information control and develops an overarching strategy guiding integrated space and cyberspace operations, prioritized by global and regional information requirements. Concepts of space and cyberspace control and superiority take on new meaning and receive heightened priority, above and beyond any one theater's

[1] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (London: Oxford University Press, 1963), 115.; J.F.C. Fuller, *The Foundations of the Science of War*, (London: Hutchinson and Company, 1926), 110.

campaign requirements. In essence, the new combatant commander is considered the *supported* commander for *global information control*, a joint imperative across the spectrum of conflict.

Pragmatically, creating a new combatant command disrupts existing paradigms by way of the authorities, command relationships, and missions given to its components. Using the space infrastructure as an example, the space component (i.e., JFCC SPACE) now operates within the appropriate *authorities* and warfighting *strategy* to devise and orchestrate space control operations *across multiple combatant commands*, as described in Chapter 5.[2] In this structure, JFCC SPACE maintains authority to coordinate with and *direct* theater commands supporting space control measures in the terrestrial segment—for both defensive (control) and offensive (superiority) missions—in support of a larger information control strategy. Likewise, JFCC SPACE and its cyber counterpart (i.e., JFCC CYBER) operate within a common framework to prioritize and execute information control operations in and through their respective domains, supported by theater combatant commands as required.

In so doing, the joint force may take a significant step in its transformation from an Industrial Age military to an Information Age force. The transition point exists in the universal acceptance of a new paradigm that places global information control at the pinnacle of warfighting. Once accepted, prevailing strategies, assumptions, expectations, objectives, structures, and priorities may then be reassessed by virtue of their ability to secure US interests in an information-driven world. Adoption of the new paradigm manifests itself in development of an information control strategy, devised and orchestrated by a new combatant command, to preserve the US military's desired way of warfare and ultimately national security in the twenty-first century.

Areas for Further Research

The theoretical framework contained within poses concepts that challenge existing notions of warfare. As a result, a few considerations were not fully explored and therefore necessitate further investigation. Four prominent areas deserve additional

[2] In this regard, the new JFCC SPACE is related to the existing JFCC SPACE in name only. Given its new authorities, strategy, and missions, the new JFCC SPACE is a completely different entity.

attention in particular. The first and perhaps most impending area involves the examination of a cyberspace control methodology that complements the space and information control concepts presented within. Relatedly, the second area involves the nuances associated with the proposed functional combatant command and how it orchestrates space and cyberspace operations in pursuit of information control. Specifically, research is needed to better understand its implications on joint and service structures, relationships, funding, and manpower (perhaps through a comprehensive DOTMLPF analysis). Third, as noted, investigation is needed on the ability for the intelligence apparatus to support an undertaking of this magnitude. What intelligence requirements stem from a global information control strategy? Will the intelligence community need to reorganize or acquire new systems to properly support the proposed methodology for space control? What is the resultant organizational relationship between the Director of National Intelligence (DNI) and the new combatant commander? Finally, adoption of an information control strategy invariably drives interactions with civil and commercial agencies. Properly infusing information control strategies between military, intelligence, civil, and commercial entities is a critical step in transforming the US defense apparatus into an Information Age power and maintaining a decided advantage in the future.

As a final note, infospheres are now indispensible to diplomacy, commerce, defense, and overall security. Furthermore, infospheres are man-made environments, creating a profound consideration for strategists: unlike natural domains, their existence is not inevitable. Hence, all national security endeavors must first account for their availability. The US military's solemn duty to *prepare for* and, if required, exert violence on behalf of the state includes the responsibility for preserving its ability to operate as desired (and authorized). In the Information Age, that responsibility extends to the deliberate identification and protection of the infospheres that make national defense endeavors possible—a fundamental characteristic of information control and Information Age warfare.

Thus, historical debates as to the military's proper role in space are quickly losing their relevance. If the United States seeks to preserve its desired way of warfare, then

inhibiting the development of a space control strategy is not only detrimental, it is irresponsible. Space control—a defensive proposition in the proposed model—adheres with the essence of strategy, conflict, and war, as space-based capabilities now hold an inseparable relationship with national and military ventures. Indeed, a comprehensive space control strategy is an essential component for establishing global information control, a foundational requirement for national security in the twenty-first century.

BIBLIOGRAPHY

Academic Papers

AU-18. *Space Primer*. Montgomery, AL: Air University Press, 2012.

Fadok, Maj David S. *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis*. Maxwell AFB, AL: Air University Press, 1994.

Forest, Benjamin D. "An Analysis of Military Use of Commercial Satellite Communications." Master's Thesis, Naval Post Graduate School. Monterey, CA, September 2008.

Mastalir, Lt Col Anthony J. *The US Response to China's ASAT Test*. Maxwell AFB, AL: Air University Press, 2009.

Sweeney, Patrick C. *A Primer for: Guidance for the Employment of Force (GEF), Joint Strategic Capabilities Plan (JSCP), the Adaptive Planning and Execution (APEX) System and Global Force Management (GFM)*. Providence, RI: Naval War College, 2011.

Books

Bergerud, Eric. *Fire in the Sky: The Air War in the South Pacific*. Boulder, CO: Westview Press, 2000.

Brauer, Jurgen, and Hubert Van Tuyll. *Castles, Battles, and Bombs: How Economics Explains Military History*. Chicago, IL: The University of Chicago Press, 2008.

Brugioni, Dino A. *Eyes in the Sky: Eisenhower, the CIA, and Cold War Aerial Espionage*. Annapolis, MD: Naval Institute Press, 2010.

Bungay, Stephen. *The Most Dangerous Enemy: An Illustrated History of the Battle of Britain*. Zenith Press, 2010.

Burrows, William E. *This New Ocean: The Story of the First Space Age*. New York, NY: The Modern Library, 1998.

Christensen, Clayton M. *The Innovator's DNA: Mastering the Five Skills of Disruptive Innovators*. Boston, MA: Harvard Business Review Press, 2011.

Clarke, Richard A. and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York, NY: Harper Collins, 2010.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Cohen, Eliot A. *Supreme Command: Soldiers, Statesmen, and Leadership in Wartime*. New York, NY: Anchor Books, 2002.

Cox, Donald and Michael Stoiko. *Spacepower: What it Means to You*. Philadelphia, PA: The John C. Winston Company, 1958.

Creveld, Martin Van. *Command in War*. Cambridge, MA: Harvard University Press, 1987.

Dolman, Everett C. *Astropolitik: Classical Geopolitics in the Space Age*. London: Frank Cass, 2002.

Dolman, Everett C. *Pure Strategy: Power and Principle in the Space and Information Age*. New York: NY, Frank Cass, 2005.

Dyson, George. *Turing's Cathedral: The Origins of the Digital Universe*. New York, NY: Vintage Books, 2012.

Fuller, J.F.C. *The Foundations of the Science of War*. London: Hutchinson and Company, 1926.

Gleick, James. *The Information: A History, A Theory, A Flood*. New York, NY: Vintage Books, 2011.

Gray, Colin S. *Modern Strategy*. New York, NY: Oxford University Press, 1999.

Heppenheimer, T. A. *Countdown: A History of Space Flight*. New York, NY: John Wiley and Sons, 1997.

Henriksen, Dag. *NATO's Gamble: Combining Diplomacy and Airpower in the Kosovo Crisis 1998-1999*. Annapolis, MD: Naval Institute Press, 2007.

Horgan, John. *The End of War*. San Francisco, CA: McSweeney's, 2014.

Howard, Michael. *War in European History*. Oxford: Oxford University Press, 1976.

Isserson, G. "The Evolution of Operational Art." In *The Evolution of Soviet Operational Art, 1927-1991: The Documentary Basis*, Vol. 1. *Operational Art, 1927-1964*. trans. Harold S. Orentstein. London: Frank Cass, 1995.

Kennett, Lee. *The First Air War: 1914-1918*. New York, NY: The Free Press, 1991.

Lambakis, Steven. *On the Edge of the Earth: The Future of American Space Power*. Lexington, KY: The University Press of Kentucky, 2001.

Lambeth, Benjamin S. *Mastering the Ultimate High Ground: Next Steps in the Military Uses of Space*. Santa Monica, CA: RAND Report, 2003.

Lambeth, Benjamin S. *The Unseen War: Allied Air Power and the Takedown of Saddam Hussein*. Annapolis, MD: Naval Institute Press, 2013.

Launius, Roger D. *NASA: A History of the U.S. Civil Space Program*. Malabar, FL: Krieger Publishing Company, 1994.

Libicki, Martin, and Jeremy Shapiro. *The Changing Role of Information in Warfare*. RAND: Project Air Force, 1999.

Liddell Hart, B.H. *Strategy*. 2nd rev. ed. 1967. Reprint: New York, NY: Penguin, 1991.

Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future*. New York, NY: Frank Cass, 2004.

McDougall, Walter A. *The Heavens and the Earth: A Political History of the Space Age*. Baltimore, MD: The Johns Hopkins University Press, 1985.

Moltz, James Clay. *The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests*. Stanford, CA: Stanford University Press, 2008.

Moore, Michael. *Twilight War: The Folly of U.S. Space Dominance*. Oakland, CA: The Independent Institute, 2008.

Nardin, Terry, and David R. Mapel, eds. *Traditions of International Ethics*. Cambridge: Cambridge University Press, 1992.

Olsen, John Andreas. *John Warden and the Renaissance of American Air Power*. Washington, DC: Potomac Books, Inc., 2007.

Osinga, Frans P.B. *Science, Strategy and War: The Strategic Theory of John Boyd*. London: Routledge, 2007.

Posen, Barry. *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars*. Ithaca, NY: Cornell University Press, 1984.

Reilly, Jeffrey M., Phd. *Operational Design: Distilling Clarity from Complexity for Decisive Action*. Maxwell AFB, AL: Air University Press, 2012.

Rosen, Stephen. *Winning the Next War: Innovation in the Modern Military*. Ithaca, NY: Cornell University Press, 1991.

Shimko, Keith L. *The Iraq Wars and America's Military Revolution*. New York, NY: Cambridge University Press, 2010.

Singer, P.W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York, NY: Oxford University Press, 2014.

Smith, Merritt Roe, and Leo Marx, eds. *Does Technology Drive History?: The Dilemma of Technological Determinism*. Cambridge, MA: The MIT Press, 1994.

Sterner, Eric, ed. *America's Space Futures: Defining Goals for Space Exploration*. The George C. Marshall Institute, 2013.

Taubman, Philip. *Secret Empire: Eisenhower, the CIA, and the Hidden Story of America's Space Espionage*. New York, NY: Simon and Schuster, 2003.

Terrill, Jr., Delbert R. *The Air Force Role in Developing International Outer Space Law*. Maxwell Air Force Base, AL: Air University Press, 1999.

Thucydides, Robert B. Strassler, Richard Crawley, and Victor Davis Hanson. *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War; with Maps, Annotations, Appendices, and Encyclopedic Index*. A newly rev. ed. of the Richard Crawley trans. New York, NY: Simon and Schuster, 1998.

Tzu, Sun. *The Art of War*. Translated by Samuel B. Griffith. London: Oxford University Press, 1963.

Wylie, Joseph. *Military Strategy: A General Theory of Power Control*. Annapolis, MD: Naval Institute Press, 1989.

Waltz, Kenneth N. *Man, the State, and War: A Theoretical Analysis*. New York, NY: Columbia University Press, 1954.

Waltz, Kenneth N. *Theory of International Politics*. Long Grove, IL: Waveland Press, Inc., 1979.

Briefings

Dolman, Everett C. "Astropolitik: A Case for Weapons in Space." Lecture. USAF School of Advanced Air and Space Studies, Maxwell AFB, AL, 16 March 2015.

Declassified Sources

Camron, Robert M., et al. *New Horizons, Volume V: Role of the Air Force in Space*. Washington, DC: HQ USAF, 1975. Document is now declassified.

Electronic Publications

Internet World Stats, "Internet Growth Statistics: And the 'Global Village' Became a Reality," http://www.internetworldstats.com/emarketing.htm (accessed 25 February 2015).

Marshall, Sergeant First Class Tyrone C., Jr. "Officials Update Congress on Military Space Policy, Challenges." American Forces Press Service, 12 March 2014. http://www.defense.gov/news/newsarticle.aspx?id=121826 (accessed 12 April 2015).

US Army Capabilities Integration Center. "What is DOTMLPF?" http://www.arcic.army.mil/AboutARCIC/dotmlpf.aspx (accessed 23 April 2015).

Welsh III, General Mark A. *Global Vigilance, Global Reach, Global Power for America*. United States Air Force, 22 Aug 2013; 2 min., 5 sec. https://www.youtube.com/watch?v=ZvWkNGr8RiQ (accessed 21 March 2015).

Government Documents

Air Force Doctrine Document 3-14. *Space Operations*. 19 June 2012.

Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 15 December 2014.

Joint Publication 3-0. *Joint Operations*. 11 August 2011.

Joint Publication 3-12(R). *Cyberspace Operations*. 5 February 2013.

Joint Publication 3-13. *Information Operations*. 20 November 2014.

Joint Publication 3-14. *Space Operations*. 29 May 2013.

Joint Publication 5-0. *Joint Operation Planning*. 11 August 2011.

Joint Publication 6-0. *Joint Communications System*. 10 June 2010.

Joint Staff, J7 JETD. Joint Officer Handbook, Staffing and Action Guide, 2d Ed., August 2011.

United States Joint Forces Command. *The Joint Operating Environment 2010*. Suffolk, VA: Joint Futures Group, February 2010.

United States Department of Defense. *National Security Space Strategy*. Washington, DC: Office of the Secretary of Defense, January 2011.

United States Department of State. “Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies.” 27 January 1967. http://www.state.gov/t/isn/5181.htm (accessed 13 November 2014).

United States Air Force. *FY 2013 Budget Overview*. Washington, DC: Office of the Deputy Assistant Secretary of the Air Force (Budget), February 2012.

United States Air Force Space Command. “16 SPCS Fact Sheet.” http://www.peterson.af.mil/library/factsheets/factsheet.asp?id=8403 (accessed 25 April 2015).

United States Air Force Space Command. “4 SPCS Fact Sheet.” http://www.peterson.af.mil/library/factsheets/factsheet.asp?id=4707 (accessed 25 April 2015).

United States Air Force Space Command. *Air Force Space Command Almanac 2004-2005*. Peterson AFB, CO: HQ Air Force Space Command, 2005.

United States Air Force Space Command. “Milstar Fact Sheet.” http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5328 (accessed 12 April 2015).

United States Strategic Command. “JFCC SPACE Fact Sheet.” http://www.vandenberg.af.mil/library/factsheets/factsheet.asp?id=12579 (accessed 25 April 2015).

United States Strategic Command. “United States Cyber Command Fact Sheet” http://www.stratcom.mil/factsheets/2/Cyber_Command (accessed 23 March 2015).

White House. *National Security Strategy.* Washington, DC: White House, 2015.

Periodicals

Cheng, Dean. “China’s Military Role in Space.” *Strategic Studies Quarterly*, Spring 2012: 55-77.

“The Synergy of Air and Space.” *Airpower Journal*, Summer 1998: 7.

Reports

Alberts, David S., John J. Garstka, Richard E. Hayes, and David A. Signori. *Understanding Information Age Warfare*. Washington, DC: DoD Command and Control Research Program, 2001.

Feickert, Andrew. *The Unified Command Plan and Combatant Commands: Background and Issues for Congress*. Washington, DC: Congressional Research Service, 2013.

Morgan, Forrest E. *Deterrence and First-Strike Stability in Space: A Preliminary Assessment*. Santa Monica, CA: RAND, 2010.

Pillsbury, Michael. *An Assessment of China's Anti-Satellite and Space Warfare Programs, Policies, and Doctrines*. Report to U.S. – China Economic and Security Review Commission, 19 January 2007.

Rothrock, John E., Edward F. Smith, Jr., and John F. Kreis. *The Industrial Age Versus the Information Age: Rethinking National Security in the 21st Century*. IDA Document D-2536. Alexandria, VA: Institute for Defense Analyses, 2001.